PATENT ABSTRACTS OF JAPAN
(11)Publication number : 2000-196585
(43)Date of publication of application : 14.07.2000

---

(51)Int.Cl. H04L 9/14
G11B 19/02
G11B 19/04
G11B 20/10

---

(21)Application number : 11-287365 (71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

(22)Date of filing : 07.10.1999 (72)Inventor : TAGAWA KENJI
MINAMI MASANAO
KOZUKA MASAYUKI
AOYAMA SHOICHI
TOKUDA KATSUMI
HIRATA NOBORU

---

30)Priority
Priority number : 10286177
10297159
10297142
Priority date : 08.10.1998
19.10.1998
19.10.1998
Priority country : JP
JP
JP

---

(54) RECORDING MEDIUM RECORDING CONTENTS, DIGITAL DATA RECORDER, DIGITAL DATA REPRODUCER, CONTENTS PACKAGING DEVICE GENERATING PACKAGE, CONTENTS REPRODUCER, COMPUTER READABLE RECORDING MEDIUM, RECORDING METHOD, REPRODUCING METHOD, PACKAGING METHOD AND SYSTEM TRANSPORT STREAM PROCESSOR CONSISTING OF CONTENTS PACKAGING DEVICE AND CONTENTS REPRODUCER

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a recording medium by which, to a consumer having purchased music contents, music contents relating to the music contents one sold at low cost and readily even when an infrastructure to realize electronic music distribution is not arranged.
SOLUTION: A recording medium records contents of purpose of sale and also records super distribution contents 10 that are encrypted on the basis of the block encryption method. A super distribution header 9 given to the super distribution contents 10 is encrypted on the basis of the encryption method that is an application of a public key and includes a decoding key 13 to decode the encryption of the block encryption method. In the case that the recording medium is loaded to a device connected to a communication channel, the encryption method that is an application of the public key can be decoded by the device and the decoding of the encryption is attended with charging through the communication channel.

CLAIMS

[Claim(s)]
[Claim 1]The 1st contents and the 2nd contents that the 1st contents are different contents and are enciphered based on the 1st cipher system, The 1st key information used in order to be matched with the 2nd contents and to make encryption in the 2nd contents cancel is included, A recording medium only when the 2nd key information beforehand distributed to a predetermined device is used, wherein a header enciphered with the 2nd cipher system that is a cipher system with which release of the encryption is performed is recorded.

[Claim 2]The recording medium comprising according to claim 1:
Said predetermined device has the function to charge. Does said header permit reproduction of the 2nd contents, or record to other recording media further or not?
Use limitation information which shows upper limit frequency in a case of permitting reproduction or record to other recording media.
Accounting information which shows a fee which record to a fee or other recording media which reproduction which should be made to charge said predetermined device takes when record is permitted by reproduction or other recording media of the 2nd contents takes.

[Claim 3]The recording medium comprising according to claim 1:
Said predetermined device has the function to charge. Does said header permit reproduction of the 2nd contents, or record to other recording media further or not?
Permission period information which shows a permission period in a case of permitting record to reproduction or other recording media.
Accounting information which shows a fee which record to a fee or other recording media which reproduction which should be made to charge said predetermined device takes when record is permitted by reproduction or other recording media of the 2nd contents takes.

[Claim 4]The recording medium according to claim 1, wherein said 1st contents are enciphered using identification information peculiar to a recording medium.
[Claim 5]A digital data recorder which records digital data containing contents on a recording medium, comprising:
A storing means which stores at least one or more contents which should be recorded on a recording medium.
A selecting means which chooses the contents as superdistribution contents when what should charge record to the reproduction or other recording media exists in said one or more contents.
The 1st encoding means that enciphers superdistribution contents based on the 1st cipher system so that reproduction about selected superdistribution contents or record to other recording media may be prevented, while fee collection is not performed.
A creating means which generates a superdistribution header including key information of which encryption of superdistribution contents is made to cancel, The 2nd encoding means that enciphers based on the 2nd cipher system whose safety is

higher than said 1st cipher system, and gives a generated superdistribution header to superdistribution contents, and a recording device which will be recorded on a recording medium by using one or more contents as digital data if a superdistribution header is given.

[Claim 6]The digital data recorder comprising according to claim 5:
An extraction means which takes out identification information in which said digital data recorder is still more peculiar to a recording medium from a recording medium.
The 3rd encoding means enciphered about contents other than superdistribution contents using identification information taken out by an extraction means.

[Claim 7]Fee collection is required for record to other recording media characterized by comprising the following, A digital data recorder which reads superdistribution contents which are contents enciphered in order to prevent what recorded on other recording media while fee collection is not performed from the 1st recording medium, and is recorded on the 2nd recording medium.
Charger stage loaded with either [at least] the 1st recording medium or the 2nd recording medium.
A reading means which will read superdistribution contents from the 1st recording medium if a recording medium with which a charger stage was loaded is the 1st recording medium.
A presenting means which shows an operator a remuneration to record to the 2nd recording medium of superdistribution contents.
A release means of which encryption of superdistribution contents read from the 1st recording medium is canceled when operation which a receiving means which receives operation from an operator, and a receiving means received is operation of a purport that it agrees with payment of a remuneration, If a charging means charged to an operator and a charger stage are loaded with the 2nd recording medium used as an archive destination of superdistribution contents when directions of a purport that it agrees with payment of a remuneration are received from an operator, A recording device recorded on the 2nd recording medium of an archive destination by using as digital data superdistribution contents of which encryption was canceled.

[Claim 8]The digital data recorder according to claim 7 which is provided with the following and characterized by said recording device recording superdistribution contents again enciphered by re-encoding means on the 2nd recording medium of an

archive destination.
An extraction means by which said digital data recorder will take out identification information peculiar to a recording medium from the 2nd recording medium used as an archive destination if a charger stage is further loaded with the 2nd recording medium used as an archive destination of superdistribution contents.
A re-encoding means enciphered again using identification information from which an extraction means took out superdistribution contents of which encryption was canceled by a release means as an encryption key.

[Claim 9]Digital data playback equipment which reproduces superdistribution contents which are contents enciphered in order to prevent reproduction [fee collection is required for the reproduction characterized by comprising the following and fee collection is not performed] of a between.
Charger stage loaded with a recording medium.
A reading means which will read this if superdistribution contents are recorded on a recording medium with which a charger stage was loaded.
A presenting means which shows an operator a remuneration to reproduction of superdistribution contents.
A release means of which encryption of superdistribution contents is canceled when operation which a receiving means which receives operation from an operator, and a receiving means received is operation of a purport that it agrees with payment of a remuneration, A charging means charged to an operator when directions of a purport that it agrees with payment of a remuneration are received from an operator, and a reproduction means which reproduces superdistribution contents of which encryption was canceled.

[Claim 10]A contents packaging device comprising:
An encoding means which is a contents packaging device which creates a package containing two or more contents, and obtains two or more contents from which quality at the time of reproduction differs by coding a candidate for distribution by a different method.
A rank means to rank each contents according to height of quality of a recycled article.
Two or more ranks.
A conversion table storing means which stores a conversion table which made a group an encryption key and a cryptographic algorithm which should be used in order to

encipher contents of each rank, An encoding means which enciphers contents to which a rank was given using an encryption key and an encryption algorithm according to a rank shown in a conversion table, and a packing means to generate a package containing said two or more enciphered contents.

[Claim 11]The contents packaging device according to claim 10 making said rank information, an encryption key, and a cryptographic algorithm into a group, and storing said conversion table storing means so that a code with high safety may be used for contents reproduced in said high quality.
[Claim 12]A contents packaging device comprising:
An encoding means which is a contents packaging device which creates a package containing two or more contents, and contents for sample offer are obtained by coding a part for distribution, and obtains difference contents by coding the remaining portion for distribution.
A rank means to give a predetermined rank to contents for sample offer, and to give a higher rank to difference contents.
Two or more ranks.
Are making into a group an encryption key and a cryptographic algorithm which should be used in order to encipher contents of each rank, and in one group. It is matched by predetermined rank and for another side to construct, A conversion table storing means which stores a conversion table matched with a rank higher than the predetermined rank concerned, An encoding means which enciphers contents to which a rank was given using an encryption key and an encryption algorithm according to a rank shown in a conversion table, and a packing means to generate a package containing said two or more enciphered contents.

[Claim 13]A contents playback device which takes out contents from a package and is reproduced, comprising:
Evaluation methods which compute a rank estimator which evaluates performance of hardware of playback equipment and shows performance of the hardware concerned.
Two or more rank estimators.
A conversion table storing means which stores a conversion table which a decode key which should be used for the encryption release processing, and a decoding algorithm constructed, and matched ** when hardware which has the performance corresponding to each rank estimator performed encryption release processing.
An acquisition means which acquires a package which each includes for two or more

contents by which encryption was made from the device exterior, Choose a thing according to a rank estimator evaluated by evaluation methods among two or more decode keys and decoding algorithms which can be set to a conversion table, and. A release means which takes out from a package contents of which encryption should be canceled in this decode key and decoding algorithm and of which encryption of taken-out contents is canceled.

[Claim 14]Contents for sample offer obtained by coding a part for [characterized by comprising the following] distribution, A contents playback device which codes the remaining portion for distribution, takes out contents from a package containing difference contents obtained by enciphering in an encryption key and a cryptographic algorithm whose safety is higher than contents for sample offer, and is reproduced.
Evaluation methods which compute a rank estimator which evaluates performance of hardware of playback equipment and shows performance of the hardware concerned.
A conversion table storing means which stores a conversion table which matches with a low rank estimator a decode key and a decoding algorithm which can cancel encryption of contents for sample offer, and matched with a high rank estimator a decode key and a decoding algorithm which can cancel encryption of difference contents.
An acquisition means which acquires a package which each includes for two or more contents by which encryption was made from the device exterior.
Choose a thing corresponding to a rank estimator evaluated by evaluation methods among two or more decode keys and decoding algorithms which can be set to a conversion table, and. A release means which takes out either one of contents for sample offer, and difference contents, and cancels encryption of taken-out contents of an acquired package.

[Claim 15]Contents for sample offer enciphered in a predetermined encryption key and a predetermined encryption algorithm, A recording medium, wherein contents for sale which were reproduced in quality higher than contents for sample offer, and were enciphered in an encryption key, an encryption key whose safety is higher than said predetermined encryption algorithm, and an encryption algorithm predetermined [said] are recorded.
[Claim 16]Contents for sample offer obtained by enciphering in a predetermined encryption key and a predetermined encryption algorithm after coding a part for distribution, A recording medium, wherein difference contents are recorded by

enciphering in an encryption key, an encryption key whose safety is higher than said predetermined encryption algorithm, and an encryption algorithm predetermined [said] after coding the remaining portion for distribution.

[Claim 17]A system comprising:

A contents packaging device which creates a package containing two or more contents.

An encoding means which is a system which consists of a contents playback device which takes out contents from a package and is reproduced, and obtains two or more contents from which quality at the time of reproduction differs when said contents packaging device codes a candidate for distribution by a different method.

A rank means to rank each contents according to height of quality of a recycled article.

Store a conversion table which made a group two or more ranks, and an encryption key and a cryptographic algorithm which should be used in order to encipher contents of each rank, and in one group. It is matched by predetermined rank and for another side to construct, The 1st conversion table storing means which stores a conversion table matched with a rank higher than the predetermined rank concerned, An encoding means which enciphers contents to which a rank was given using an encryption key and an encryption algorithm according to a rank shown in a conversion table, Have a packing means to generate a package containing said two or more enciphered contents, and said contents playback device, Evaluation methods which compute a rank estimator which evaluates performance of hardware of playback equipment and shows performance of the hardware concerned, The 2nd conversion table storing means which stores a conversion table which matched a decode key and a decoding algorithm which should be used for the encryption release processing when hardware which has the performance corresponding to two or more rank estimator and each rank estimator performed encryption release processing, Two or more decode keys which can set a package whose each contains two or more contents by which encryption was made to an acquisition means acquired from the device exterior, and a conversion table, and inside of a decoding algorithm, A release means which takes out from a package contents of which encryption should be canceled in this decode key and decoding algorithm and of which a thing according to a rank estimator evaluated by evaluation methods is chosen, and encryption of taken-out contents is canceled.

[Claim 18]A recording medium which a computer with a storage which stores at least one or more contents can read, comprising:

A selection step which chooses the contents as superdistribution contents when what should charge record to the reproduction or other recording media exists in said one or more contents.
The 1st encryption step which enciphers superdistribution contents based on the 1st cipher system so that reproduction about selected superdistribution contents or record to other recording media may be prevented, while fee collection is not performed.
A generation step which generates a superdistribution header including key information of which encryption of superdistribution contents is made to cancel.
The 2nd encryption step which enciphers based on the 2nd cipher system whose safety is higher than said 1st cipher system, and gives a generated superdistribution header to superdistribution contents, and a record step which will be recorded on a recording medium by using one or more contents as digital data if a superdistribution header is given.

[Claim 19]The 1st recording medium and a recording medium which a computer with a loading section loaded with either of the 2nd recording medium can read characterized by comprising the following.
A read-out step which will read this from the 1st recording medium if a loading section is loaded with the 1st recording medium with which superdistribution contents enciphered in order to prevent what recorded on other recording media while fee collection is not performed were recorded.
A presentation step which shows an operator a remuneration to record to the 2nd recording medium of superdistribution contents.
A reception step which receives operation from an operator.
A release step of which encryption of superdistribution contents read from the 1st recording medium is canceled when operation which a reception step received is operation of a purport that it agrees with payment of a remuneration, If it is loaded with a fee collection step charged to an operator, and the 2nd recording medium that becomes a loading section with an archive destination of superdistribution contents when directions of a purport that it agrees with payment of a remuneration are received from an operator, A record step recorded on the 2nd recording medium of an archive destination by using as digital data superdistribution contents of which encryption was canceled.

[Claim 20]A recording medium which a computer with a loading section loaded with a

recording medium can read, comprising:
A read-out step which will read superdistribution contents if a loading section is loaded with a recording medium with which superdistribution contents which fee collection is required for the reproduction, and are enciphered in order to prevent reproduction [fee collection is not performed] of a between were recorded.
A presentation step which shows an operator a remuneration to reproduction of superdistribution contents.
A reception step which receives operation from an operator.
A release step of which encryption of superdistribution contents is canceled when operation which a reception step received is operation of a purport that it agrees with payment of a remuneration, A fee collection step charged to an operator when directions of a purport that it agrees with payment of a remuneration are received from an operator, and regeneration steps which will reproduce superdistribution contents of which encryption was canceled if fee collection is performed to an operator.

[Claim 21]A recording medium which a computer with a conversion table storage which stores a conversion table which made a group two or more ranks characterized by comprising the following, and an encryption key and a cryptographic algorithm which should be used in order to encipher contents of each rank can read.
A coding step which obtains two or more contents from which quality at the time of reproduction differs by coding a candidate for distribution by a different method.
A rank, a ** step which rank each contents according to height of quality of a recycled article.
An encryption step which enciphers contents to which a rank was given using an encryption key and an encryption algorithm according to a rank shown in a conversion table.
A packing step which generates a package containing said two or more enciphered contents.

[Claim 22]A recording medium which a computer with a storage which stores a conversion table which made a group two or more ranks characterized by comprising the following, and an encryption key and a cryptographic algorithm which should be used in order to encipher contents of each rank can read.
Said coding step which contents for sample offer are obtained by coding a part for distribution, and obtains difference contents by coding the remaining portion for

distribution.
A rank step which gives a predetermined rank to contents for sample offer, and gives a higher rank to difference contents.
An encryption step which enciphers contents to which a rank was given using an encryption key and an encryption algorithm according to a rank shown in a conversion table.
A packing step which generates a package containing said two or more enciphered contents.

[Claim 23]Two or more rank estimators.
Performance corresponding to each rank estimator.
Are the recording medium provided with the above in which computer reading is possible, and performance of hardware of a computer is evaluated, An evaluation step which computes a rank estimator which shows performance of the hardware concerned, An acquisition step which acquires a package which each includes for two or more contents by which encryption was made from the computer exterior, Choose a thing according to a rank estimator evaluated by an evaluation step among two or more decode keys and decoding algorithms which can be set to a conversion table, and. A packaging program to which a procedure which consists of a release step which takes out from a package contents of which encryption should be canceled in this decode key and decoding algorithm, and of which encryption of taken-out contents is canceled is made to follow to a computer is recorded.

[Claim 24]A record method with which a computer with a storage which stores at least one or more contents which should be recorded on a recording medium records digital data containing contents on a recording medium, comprising:
A selection step which chooses the contents as superdistribution contents when what should charge record to the reproduction or other recording media exists in said one or more contents.
The 1st encryption step which enciphers superdistribution contents based on the 1st cipher system so that reproduction about selected superdistribution contents or record to other recording media may be prevented, while fee collection is not performed.
A generation step which generates a superdistribution header including key information of which encryption of superdistribution contents is made to cancel.
The 2nd encryption step which enciphers based on the 2nd cipher system whose

safety is higher than said 1st cipher system, and gives a generated superdistribution header to superdistribution contents, and a record step which will be recorded on a recording medium by using one or more contents as digital data if a superdistribution header is given.

[Claim 25]A record method which records digital data containing superdistribution contents which said record method was applied to a computer with a loading section which loads with any of the 1st recording medium and the 2nd recording medium they are, and were recorded on the 1st recording medium on the 2nd recording medium, comprising:
A read-out step which will read this from the 1st recording medium if a loading section is loaded with the 1st recording medium with which superdistribution contents enciphered in order to prevent what recorded on the 2nd recording medium while fee collection is required for record to the 2nd recording medium and fee collection is not performed were recorded.
A presentation step which shows an operator a remuneration to record to the 2nd recording medium of superdistribution contents.
A reception step which receives operation from an operator.
A release step of which encryption of superdistribution contents read from the 1st recording medium is canceled when operation which a reception step received is operation of a purport that it agrees with payment of a remuneration, If it is loaded with a fee collection step charged to an operator, and the 2nd recording medium that becomes a loading section with an archive destination of superdistribution contents when directions of a purport that it agrees with payment of a remuneration are received from an operator, A recording device recorded on the 2nd recording medium of an archive destination by using as digital data superdistribution contents of which encryption was canceled.

[Claim 26]A regeneration method which reproduces digital data which is applied to a computer with a loading section loaded with a recording medium, and is recorded on a recording medium, comprising:
A read-out step which will read this if superdistribution contents enciphered in order to prevent reproduction [fee collection is required for the reproduction and fee collection is not performed to a recording medium with which a loading section was loaded] of a between are recorded.
A presentation step which shows an operator a remuneration to reproduction of

superdistribution contents.
A reception step which receives operation from an operator.
A release step of which encryption of superdistribution contents is canceled when operation which a reception step received is operation of a purport that it agrees with payment of a remuneration, A fee collection step charged to an operator when directions of a purport that it agrees with payment of a remuneration are received from an operator, and regeneration steps which will carry out re-[of the superdistribution contents of which encryption was canceled] if fee collection is performed to an operator.

[Claim 27]It is applied to a computer with a conversion table storage which stores a conversion table which made a group two or more ranks characterized by comprising the following, and an encryption key and a cryptographic algorithm which should be used in order to encipher contents of each rank, A contents packaging method which creates a package containing two or more contents.
A coding step which obtains two or more contents from which quality at the time of reproduction differs by coding a candidate for distribution by a different method.
A rank, a ** step which rank each contents according to height of quality of a recycled article.
An encryption step which enciphers contents to which a rank was given using an encryption key and an encryption algorithm according to a rank shown in a conversion table.
A packing step which generates a package containing said two or more enciphered contents.

[Claim 28]It is applied to a computer with a storage which stores a conversion table which made a group two or more ranks characterized by comprising the following, and an encryption key and a cryptographic algorithm which should be used in order to encipher contents of each rank, A contents packaging method which creates a package containing two or more contents.
Said coding step which contents for sample offer are obtained by coding a part for distribution, and obtains difference contents by coding the remaining portion for distribution.
A rank, a ** step which give a predetermined rank to contents for sample offer, and give a higher rank to difference contents.
An encryption step which enciphers contents to which a rank was given using an

encryption key and an encryption algorithm according to a rank shown in a conversion table.
A packing step which generates a package containing said two or more enciphered contents.

[Claim 29]Two or more rank estimators.
Performance corresponding to each rank estimator.
Are the regeneration method provided with the above and performance of hardware of a computer is evaluated, An evaluation step which computes a rank estimator which shows performance of the hardware concerned, An acquisition step which acquires a package which each includes for two or more contents by which encryption was made from the computer exterior, Choose a thing according to a rank estimator evaluated by an evaluation step among two or more decode keys and decoding algorithms which can be set to a conversion table, and. A procedure which consists of a release step which takes out from a package contents of which encryption should be canceled in this decode key and decoding algorithm, and of which encryption of taken-out contents is canceled is made to follow to a computer.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]The recording medium which recorded the contents which make the start the musical works; by which this invention was digitized, It is related with the device which records contents on a recording medium, the device which reproduces the contents currently recorded on the recording medium, the device

which carries out packaging of two or more contents, the recording medium in which computer reading is possible, a record method, a regeneration method, and a packaging method.

[0002]

[Description of the Prior Art](The 1st conventional technology) It argues about how there should be any sales styles of next-generation musical works; briskly between major concert companies, the audio equipment maker, and the well-informed person. With the sales styles of the present musical works;, the musical works; of various genres, such as pop, a lock, and a classic, CD, It is the gestalt of recording on recording media, such as magnetic tape, and selling, and it can be said that the life style of purchasing the recording medium sold in this way, and appreciating musical works; has permeated all over the world.

[0003]As sales styles which oppose the sales styles using a recording medium, the sales styles called electronic music distribution attract many attentions. Electronic music distribution performs charged distribution of a music content (contents say the thing of the digitized works and especially a music content says the thing of the digitized musical works;) on the Internet which shows rapid spread in recent years. The special feature of this electronic music distribution is the point that fee collection to the proposal of sale of a music content and those who purchased the music content is performed according to electronic commerce technology (Electronic Commerce). That is, in this electronic music distribution, the concert company is introducing various contents to the homepage which self opened.

Consumers can search various contents by accessing the homepage of each concert company.

When there are favorite contents, consumers notify this concert company of the purchase request of contents, operator ID, etc. The concert company can settle the purchase price of contents based on the bank account corresponding to the number of the credit card beforehand notified by the operator. After such settlement of accounts, consumers can download contents to the computer which consumers own, and can obtain their favorite contents.

[0004]Thus, since it downloads in electronic music distribution according to interactive selection operation, For example, in the homepage which sells the contents of the newly released piece of music with high name recognition, If the contents of other scores of the singer who sings the contents of other scores of the artist who wrote the lyrics for and composed the contents of the newly released piece of music, and the contents of the newly released piece of music are introduced, a

score besides these can be sold to consumers.That is, it is statistically clear that the consumers' who are going to purchase a certain artist's newly released piece of music an interest strong against the score in which the artist is related is shown, and they can promote such two or more related scores efficiently in electronic music distribution.

[0005](The 2nd conventional technology) As the 1st conventional technology described, some distribution gestalten of a music content are various at first about the sales styles using communication lines which used the recording medium, such as sales styles and the Internet. Even if it says at a recording medium and a word, there is a kind of DVD-Audio, CD, etc. of recording media, and each of these is recording the music content in the state where it was coded by a different coding mode. There are also many opportunities for a music content to be distributed, by being broadcast in broadcast waves, such as satellite broadcasting and a cable TV, besides such sales styles. Although it is a principle that these distribution is performed for counter value, it may be offered gratuitously as a sample in order to raise the notability of a music content.

[0006]When musical works; are distributed with various gestalten like a recording medium, a broadcast wave, and a communication line, even if the number of the musical works; which should be distributed even if is one, the side which distributes musical works; must create and distribute the music content of the gestalt according to each distribution gestalt. Here, it is based on the following reasons that it must code with a different coding mode. Namely, to the playback equipment which has already spread through each household, and the playback equipment which is spreading from now on. Since the height of the existence of a copyright protection mechanism and the safety of an encryption key differs for every playback equipment from the height of the quality of a recycled article of the music content at the time of reproduction, It is because there is a possibility that the ability to regenerate by which a copyright protection mechanism is not utilized at all or with which playback equipment is originally provided cannot be demonstrated even if it transmits a music content uniformly with the same coding mode.

[0007]I can think that what is necessary is just to encipher the music content distributed with all the gestalten with an encryption key with high safety if the playback equipment in which the copyright protection mechanism is already fixed exists. However, since the object for sample offer, etc. have some which are distributed for the purpose of the improvement in notability in a music content and such a music content should just be reproduced in low quality, If the music content

reproduced only in low quality such is also uniformly enciphered with an encryption key with high safety, encryption by an encryption key with such high safety must be solved to also reproduce the contents of quality low to sample offer. Now, the playback equipment which does not have the decoding capability to cancel encryption with high safety will become impossible [reproducing the contents for sample offer], and its opportunity for the contents for sample offer to be reproduced will decrease. Thus, if the opportunity for the contents for sample offer to be reproduced decreases, the advertisement action of aiming at sales promotion broadly by sample offer of a music content will lose an original target. Creating and distributing the music content of a gestalt according to each distribution gestalt for the above reason was performed inevitably.

[0008]

[Problem(s) to be Solved by the Invention]By the way, infrastructures for becoming a problem in the 1st conventional technology to realize electronic music distribution are the actual condition and the point that consumers are burdened with various burdens in order to be unable to say that it is fixed enough but for consumers to obtain a music content by electronic music distribution. Although a typical thing is a high speed line which can transmit the music content which has data size of several megabytes in a short time among the infrastructures made indispensable because of realization of electronic music distribution here, Ordinary Internet users use the Internet by accessing a server via a public line. As for the access speed of the public line which ordinary Internet users use, it is common that it is much less than the access speed of a high speed line. Thus, since hour corresponding turns into a long time when ordinary Internet users download two or more contents simultaneously as mentioned above via a low speed public line, consumers will pay a telecom company a great quantity of telex rate gold. When extreme, it is possible that the way of telex rate gold becomes high rather than the fee which consumers pay to a concert company about the purchase of contents. Thus, if consumers are burdened with a great quantity of fees, the volition of the consumers who are going to use electronic music distribution will be depressed in spirits. Since the time which the transmission in a public line takes becomes very long when transmitting two or more contents, increasing also on the problem of this fee side and feeling uneasy is the point of irritating for fun those who wished the purchase of contents. Thus, if transmission of contents excels, those who wished the purchase of contents may cancel the purchase of contents in the middle of download of two or more contents.

[0009]But in the sales styles using a recording medium like electronic music distribution, When trying to sell the contents of a related score, a selling point, the selling price, etc. are printed about such a related score in the jacket enclosed by the case which stored the recording medium, and the classic technique of recommending the purchase of a related score must be taken. Consumers obtain a related score by going to the retail store of contents, in order to purchase the related score, and purchasing the recording medium with which the related score was recorded, when got interested in a related score, seeing the printing content of such a jacket.
[0010]Various costs concerning manufacture and circulation of a recording medium are appropriated for the retail price of the recording medium currently sold to the retail store here. Therefore, when it is going to purchase the both sides of the recording medium with which the newly released piece of music was recorded, and the recording medium with which the related score was recorded, Since it is necessary to pay the retail price for which various costs concerning manufacture and circulation of these recording media were appropriated about each of two contents, consumers will pay a comparatively high-priced fee.
[0011]In the sales styles using the present recording medium, in order for consumers to obtain a related score, The consumer itself has to go to the retail store of a recording medium specially, and consumers cannot purchase a related score freely but may lose the volition which is going to purchase such a related score by the time it goes to the retail store of a recording medium. In the 2nd conventional technology, the supplier of a music content, Since it is necessary to code with a different coding mode according to a distribution gestalt, the more there are many contents coded, the more the supplier of a music content is the point of sensing great stress for management and distribution of these music contents. Thus, stress is sensed because the probability of a misdelivery-of-mail cloth, such as distributing the contents for sale and the contents for sample offer accidentally, will also become high, for example, if the number of the contents coded increases. If such a misdelivery-of-mail cloth arises, the contents for sale will flow into a public place, and if those all are not collected, the supplier of a music content will wear a great blow economically.
[0012]The 1st purpose of this invention is to provide the recording medium which can moreover sell easily the music content relevant to this music content with a low price to the consumers who purchased a certain music content, even if the infrastructure for realizing electronic music distribution has not fixed. The 2nd purpose of this invention is to provide the contents packing system which can distribute the music content to these uniformly, even if the height of the existence of a copyright

protection mechanism and the safety of an encryption key and the height of the quality of a recycled article of the music content at the time of reproduction are the cases where it differs for every playback equipment.

[0013]

[Means for Solving the Problem]The 2nd contents that the 1st purpose of the above is the 1st contents and contents from which the 1st contents differ, and are enciphered based on the 1st cipher system, The 1st key information used in order to be matched with the 2nd contents and to make encryption in the 2nd contents cancel is included, It is attained by recording medium by which a header enciphered with the 2nd cipher system that is a cipher system with which release of the encryption is performed is recorded only when the 2nd key information beforehand distributed to a predetermined device is used.

[0014]An encoding means which obtains two or more contents from which quality at the time of reproduction differs when the 2nd purpose codes a candidate for distribution by a different method, A rank means to rank each contents according to height of quality of a recycled article, A conversion table storing means which stores a conversion table which made a group two or more ranks, and an encryption key and a cryptographic algorithm which should be used in order to encipher contents of each rank, It is attained by contents packaging device provided with an encoding means which enciphers contents to which a rank was given using an encryption key and an encryption algorithm according to a rank shown in a conversion table, and a packing means to generate a package containing said two or more enciphered contents.

[0015]

[Embodiment of the Invention]The embodiment about the recording medium concerning this invention, playback equipment, and a recorder is described. Since explanation will become remarkably complicated if one embodiment tends to explain a recording medium, playback equipment, and a recorder, the above-mentioned contents shall be individually explained in a 6th embodiment from a 1st embodiment.

[0016](A 1st embodiment) A 1st embodiment explains the recording medium used for the sales use of a music content. The music content of the sales purpose is recorded on the recording medium used for the sales use of a music content, and sale of contents is made by transferring this recording medium for counter value. There are two types of recording media of such a sales use. The 1st type records the music content aiming at sale on Enhanced-CD. The disk which it has the physical structure as the usual CD (CD-DA) with same inner periphery, and the peripheral part has the same physical structure as CD-ROM, and had the function of both CD and CD-ROM

is called Enhanced-CD. The appearance of this Enhanced-CD is shown in drawing 1 (a), and the physical structure of Enhanced-CD is shown in drawing 1 (b). In drawing 1 (a), the inner periphery of Enhanced-CD is called a CD-DA part, and a peripheral part is called a CD-ROM part. When these CD-DA part and a CD-ROM part are considered functionally, a CD-DA part is the contents area 1 where the music content 3 is recorded, and a CD-ROM part is the added value field 2 which recorded the data which adds the value of main story recording media. This recording medium for sale is used for the use which sells the music content recorded on this contents area 1.

[0017]The recording medium of the sales use of the 2nd type is DVD-AUDIO on which the music content 3 of the sales purpose was recorded. The appearance of this DVD-AUDIO is shown in drawing 2 (a), and the logical format is shown in drawing 2 (b). The CD-DA part shown in this DVD-AUDIO at Enhanced-CD, Each of the sales purpose contents 3, the reproduction control script 4, the still picture data 5, and the container 6 is recorded by an accessible file with a personal computer to a CD-ROM part not existing. Thus, although it differs from Enhanced-CD in that it is recorded by a file, the functional data structure is the same as that of Enhanced-CD, and consists of the contents area 1 and the added value field 2. The point that the music content 3 is recorded on the contents area 1 in DVD-AUDIO, and the data which adds the value of main story recording media to the added value field 2 is recorded is also the same as that of Enhanced-CD. The difference from Enhanced-CD in the contents area 1 of Enhanced-CD. The music content 3 of the sales purpose currently recorded on the contents area 1 of DVD-AUDIO to the sales purpose contents 3 being recorded as it is, without also giving encryption [what] is a point enciphered using identification information peculiar to DVD-AUDIO.

[0018]Like the usual CD, these two types of recording medium for sale is stored by the plastic case for exclusive use, where a jacket and a musical score card are enclosed. Drawing 3 is a figure showing the plastic case for exclusive use which stored the recording medium for sale. If the track name of the contents currently recorded on the contents area 1 here is made into track name:OOO, as shown in drawing 3, it turns out that the photograph about track name:OOO is mainly printed at the jacket of the recording medium for sale.

[0019]In the above explanation, it became clear that the contents area 1 and the added value field 2 exist in the both sides of Enhanced-CD and DVD-AUDIO. Then, the contents of record of the added value field 2 are explained. The contents of record of the added value field 2 are shown in the right column of drawing 1 (b) and

drawing 2 (b). As shown in this figure, in the added value field 2, it turns out that the reproduction control script 4, the still picture data 5, and the container 6 are recorded.
[0020]When a device with a display function is loaded with the recording medium for this sale, the reproduction control script 4 is the information which described the contents displayed on the interactive screen of this device, and is described by Macromedia Director form and HTML form. here -- Macromedia Director form -- the utilization time of the general-purpose authoring software of MS-Windows/MacOS -- description of an authoring procedure -- business -- **** -- form -- it is -- HTML form is a form by which the object for ** is carried out to description of the Internet browser.
[0021]In the interactive screen reproduced in the reproduction control script 4, the still picture data 5 is a still picture which should be displayed. Although these reproduction control scripts 4 and the still picture data 5 exist also in conventional Enhanced-CD, the still picture data 5 and the reproduction control script 4 in this embodiment differ in a conventional thing and display information. Namely, although the words of the sales purpose contents 3, a promotion image and a fan club, newly-released-piece-of-music guidance, etc. display the information relevant to the sales purpose contents 3 on the conventional still picture data 5 and the reproduction control script 4, The still picture data 5 and the reproduction control script 4 in this embodiment display on the above-mentioned device the information which recommends purchase and reproduction of a music content which are different in the sales purpose contents 3.
[0022]For example, if it is a newly released piece of music of a popular artist with the sales purpose contents 3, the reproduction control script 4 in this embodiment will recommend purchase and reproduction of the hit song the popular artist's past. It is shown clearly by subsequent explanation what the music content to which purchase and reproduction are recommended in these reproduction control script 4 is.
[0023]Then, the container 6 in the added value field 2 included to the both sides of Enhanced-CD and DVD-AUDIO is explained. The data structure of the container 6 is shown in drawing 4. In this figure, the container 6 consists of the encryption header 7 and the enciphered content 8, the encryption header 7 contains the superdistribution header 9, and the enciphered content 8 contains the superdistribution contents 10.
[0024]It is Emeritus Professor University of Tsukuba as a "superdistribution" here. It is a circulation gestalt of the digital contents which Mr. woods Ryoichi and others recites. In a superdistribution, digital contents circulate, where the superdistribution header defined beforehand is given. At this superdistribution header, the remuneration

information about the details of the remuneration which shows the right holder who should deal in a remuneration is describing, Fare adjustment is performed, when consumers wish use of these digital contents, and the apparatus which consumers own interprets these right holder information and remuneration information and creates use record.

[0025]The superdistribution header 9 and the superdistribution contents 10 are stored in the container 6 in the form on condition of such a superdistribution, i.e., superdistribution form. Thus, the superdistribution contents 10 stored in the state where it was enciphered in the container 6 are just music contents to which purchase and reproduction are recommended in the still picture data 5 and the reproduction control script 4.

[0026]Since information, including right holder information, remuneration information, etc., important in order to perform a superdistribution safely is shown in the superdistribution header 9 as mentioned above, it is necessary to prevent malfeasances, such as an alteration of this, efficiently. Therefore, the superdistribution header 9 in this embodiment includes the data area enciphered based on the cipher system adapting a public-key-encryption algorithm (in addition, the superdistribution header 9 whole may be enciphered.). The following sentences explain as what the superdistribution header 9 whole is enciphered as. . It is known widely that there are generally kinds of public key encryption, such as a elliptic curve cryptosystem and RSA cryptograph (Rivest, Shamir, Adleman encryption). Since it is necessary to use different decode keys from the public key used for encryption in order to decode the data enciphered using these public keys, it is said that safety of a public key is very high.

[0027]However, a public key is not only used for the cipher system of public key application used when enciphering the superdistribution header 9 in this embodiment, but the following points are improved. That is, in the cipher system of the public key application in this embodiment, the decode key for solving encryption of the data area in the superdistribution header 9 is beforehand distributed to the predetermined dedicated device, and when this dedicated device is loaded with the recording medium for sale, encryption of the superdistribution header 9 is canceled. When this dedicated device is connected to the communication line in this embodiment, encryption of the superdistribution header 9 tends to be canceled and superdistribution contents tend to be reproduced, Or when superdistribution contents are recorded on other recording media, the dedicated device concerned performs fee collection through a communication line so that the right holder about superdistribution contents may get

a just remuneration. When you are going to make it record various superdistribution contents on the recording medium for sale, different public keys are used about each superdistribution header of superdistribution contents. On the other hand, a dedicated device decodes this superdistribution header using a common decode key, even if enciphered using the public key from which those superdistribution headers differ. Although a dedicated device is explained in this embodiment as what performs fee collection at the time of reproducing or buying superdistribution contents via a communication line, accounting information is recorded on another recording media, such as an IC card, and another device may perform the settlement of accounts about accounting information. Another device may perform fee collection by a prepaid card.

[0028]Since the decode key for canceling encryption of the superdistribution header 9 is formed in the dedicated device and does not exist on the recording medium for sale, Even if a person with bad faith tries to acquire the recording medium for sale and cancel encryption of this superdistribution header 9 using inaccurate apparatus, the probability that that encryption will be canceled is very low. Thus, since it is very difficult to cancel encryption of the superdistribution contents 10 unlawfully, the commercial transaction of the superdistribution contents 10 is performed safely.

[0029]If the track name of the superdistribution contents 10 is made into ******, as shown in drawing 3, no contents about ****** are printed by the jacket of the recording medium for sale. This is for ordinary consumers to prevent mistaking saying "Whether the superdistribution contents 10 are supplied gratuitously to those who purchased the sales purpose contents 3."

[0030]Then, the contents of the superdistribution header 9 are explained, referring to drawing 4. In drawing 4, the stage of most right-hand side shows the contents of the superdistribution header 9. The superdistribution header 9 comprises the content ID 11, the terms of purchase 12, and the decode key 13 so that he can understand also from here. Information for the content ID 11 to discriminate the superdistribution contents 10 from other contents is described. Since the superdistribution contents 10 are music contents, identification information, such as ISRC (International Standard Recording Code), is described as the content ID 11. ISRC is peculiar ID information uniquely assigned for every music here, and it is constituted by a country code (two ASCII characters), a record year (double digits), and the serial number (five digits).

[0031]The information concerning [the terms of purchase 12] the terms of purchase of contents is described. Here, an example of the terms of purchase 12 is shown in drawing 5. In drawing 5, refreshable upper limit is integrally described by the "number of times of reproducing permission" column. When a digital output terminal shows

whether the digital output as for which the ********** case passed this digital output terminal is permitted at a dedicated device and it permits "the number of times of digital output permission", that output time is described by the integral value.
[0032]Time, i.e., renewable time, for the "reproduction-permission-time" column to permit reproduction of contents is described. The date when the "reproducing permission date" column permits reproduction of contents is described. When the date when reproduction was permitted passes, reproduction of the contents can be performed. The "accounting information" column includes the information which shows the price at the time of acquisition of the superdistribution contents 10, or the price at the time of reproduction. Here, when the price at the time of acquisition records the superdistribution contents 10 in the container 6 on other recording media, it means the price with which an operator is burdened, and the price at the time of reproduction expresses the price according to the reproduction frequency of the specific charge 10, i.e., the superdistribution contents in the container 6. In electronic commerce technology, this accounting information is treated as a purchase applying document with a signature, and This, That a dedicated device transmits operator ID to the host computer in a charging center means that the owner of the recording medium for sale applies for the purchase of the superdistribution contents 10 in electronic commerce technology. That is, the dedicated device loaded with a recording medium transmits operator ID and this accounting information to the charging center of a concert company via a communication line, when the operator has agreed on playback of the superdistribution contents 10, or acquisition. On the other hand, since learning of an operator's bank account corresponding to [the credit card number is registered beforehand and] this card number has been beforehand carried out to the charging center of the concert company, If operator ID is transmitted, the purchase price of contents will be settled by pulling down the price shown in accounting information from the bank account corresponding to the credit card number of the operator of the transmitting origin.
[0033]The decode key 13 is a decode key for decoding the superdistribution contents 10. The superdistribution contents 10 LPCM (Linear Pulse Code Modulation) form, It is a music content of AAC (Advanced Audio Coding) form and DTS (Digital Theater System) form, and is enciphered with the block cipher system. A block cipher divides contents into every fixed length (block length) of a certain, and means the method of enciphering by the block unit, and DES (64 bits of block length are fixed), RC5 (block length is variable), etc. are equivalent to this. Since the key for decrypting with the enciphered key in this block cipher system is the same, safety is not so high as a

public key. Although the decode key 13 must be obtained to cancel encryption of the superdistribution contents 10, since the decode key 13 exists in the superdistribution header 9 firmly enciphered with the cipher system of public key application, safety is high and it is dramatically difficult to cancel encryption of the superdistribution contents 10 unlawfully. The superdistribution contents 10 will be firmly protected as a result.

[0034]Thus, since the terms of purchase 12 about the purchase of the superdistribution contents 10, etc. are included in the superdistribution header 9 enciphered in the public key with high safety, the alteration of accounting information and decoding of the superdistribution header 9 become very difficult. Since the superdistribution contents 10 are not enciphered in a public key but only the superdistribution header 9 is enciphered in the public key, in order to obtain the superdistribution contents 10, What is necessary is to cancel encryption of the superdistribution header 9, to take out the decode key 13 and just to cancel the superdistribution contents 10 using the decode key 13. Since the portion enciphered by the public key application method is limited to the header part, The part which should cancel encryption is brief, and since acquisition and time to become renewable are short and it ends after pointing to acquisition and reproduction of the superdistribution contents 10, those who wished the superdistribution contents 10 are not irritated for fun. Since it is thought that the time which this release takes becomes very shorter than the time which download of the music content in electronic music distribution takes, the operator can appreciate immediately the superdistribution contents 10 which wished acquisition or reproduction.

[0035]Then, the management information about sales purpose contents, a superdistribution header, and superdistribution contents is explained. Although sales purpose contents are managed in the management information in CD and DVD-AUDIO here, a superdistribution header and superdistribution contents are not managed in such management information. Thus, since sales purpose contents are managed in the management information in CD and DVD-AUDIO, it is recognized by a CD player and the DVD-AUDIO player (this does not mean the digital data playback equipment 400 mentioned later) as music, and are played, but. Since it is not managed in such management information, a superdistribution header and superdistribution contents are recognized by a CD player and the DVD-AUDIO player as music, and are not reproduced. If it is going to reproduce a superdistribution header and superdistribution contents as it is like sales purpose contents, a CD player and a DVD-AUDIO player this, Since a CD player and the DVD-AUDIO player will not be able to decode a

superdistribution header and superdistribution contents but a meaningless and jarring sound will be outputted, it is for a superdistribution header and superdistribution contents to avoid being reproduced like sales purpose contents such. Replace with the management information in such CD and DVD-AUDIO, and to a superdistribution header and superdistribution contents. It is managed in the peculiar management information for distinguishing self from sales purpose contents, and when a dedicated device reads a superdistribution header and superdistribution contents, the recording start position-recording end position about a superdistribution header and superdistribution contents is pinpointed in this peculiar management information.

[0036]Then, it is shown clearly how these sales purpose contents 3 and the superdistribution contents 10 spread round consumers, or how the superdistribution of the superdistribution contents 10 is performed, referring to drawing 6. Drawing 6 is a figure showing how the sales purpose contents 3 in this embodiment and the superdistribution contents 10 circulate. In drawing 6, the recording medium for sale is manufactured, when the digital data recorder 100 installed in the direct management factory of a concert company as shown in the arrow y1 records the sales purpose contents 3, the reproduction control script 4, the still picture data 5, and the container 6 on the recording medium 200. Thus, like the usual CD, the manufactured recording medium 200 for sale is sold through distribution channels, such as transportation of a track, at the shop front of a retail store, as shown in the arrow y2. Ordinary consumers can purchase the recording medium 200 for sale currently sold as shown in the arrow y3.

[0037]The consumers who purchased the recording medium 200 for sale can appreciate the sales purpose contents 3 in the usual CD and the same style as DVD-AUDIO. That is, as shown in the arrow y4 of this figure, the sales purpose contents 3 can be appreciated by reproducing playback equipment portable during a walk. In consumers' home, the digital data recorder 300 and the digital data playback equipment 400 shall be installed as a dedicated device connected to the communication line here. Among these, the digital data recorder 300 is a thing which makes the superdistribution contents 10 currently recorded on the recording medium 200 for sale record on other recording media for counter value, The digital data playback equipment 400 reproduces the superdistribution contents 10 currently recorded on the recording medium 200 for sale for counter value. The still picture data 5 currently recorded on the recording medium 200 for sale and the reproduction control script 4 display on these digital data recorder 300 and digital data playback equipment the interactive screen shown in drawing 8. Drawing 8 is a figure showing an

example of the interactive screen displayed on the display screen of playback equipment with the reproduction control script 4 and the still picture data 5. The picture m1 to which the interactive screen in drawing 8 introduces the superdistribution contents 10, such as a situation of a live performance, The message m2 of a purport which recommends reproduction of the superdistribution contents 10, and the button m3 and m13 which can specify the approval or refusal to the reproduction, It turns out that the frame m4 of a reproduction price, the character string m5 which described recommending the purchase of the score concerned, the button m6 and m16 which can specify the approval or refusal to the purchase, and its purchase price m7 are included, and it has become contents which recommend the onerous purchase of the superdistribution contents 10, and onerous reproduction. If consumers do learning of what kind of superdistribution contents 10 are recorded in the container 6 of Enhanced-CD and he is interested in them in this interactive screen, consumers, These superdistribution contents 10 can be bought using the digital data recorder 300, and these superdistribution contents 10 can be reproduced using digital data playback equipment. When the superdistribution contents 10 are bought and the superdistribution contents 10 are reproduced, the digital data recorder 300 and the digital data playback equipment 400 transmit the accounting information which shows required charge amount through a public line. The transmitted accounting information is transmitted to the host computer 600 currently installed in the charging center of a music center.

[0038]Drawing 7 (a) – drawing 7 (d) are the figures showing signs that the copy from the recording medium 200 for sale to the recording medium of an acquisition use is performed, via the digital data recorder 300. DVD-RAM shall be used as a recording medium of an acquisition use here. If the recording medium 200 for sale and the recording medium 650 of an acquisition use are set in the digital data recorder 300 in drawing 7 (a), as shown in drawing 7 (b), The operator of the digital data recorder 300 copies the works currently recorded on the recording medium 200 for sale to the recording medium 650 of an acquisition use. Then, if DVD-RAM which is the recording medium 650 of an acquisition use is ejected as shown in drawing 7 (c), acquisition of the superdistribution contents 10 will be completed. After such acquisition, if DVD-RAM is taken out from the cartridge of DVD-RAM, the contents recorded on DVD-RAM will be reproduced by using the DVD-Audio player of type corresponding to DVD-RAM. Here, the DVD-Audio player of type corresponding to DVD-RAM means the DVD-Audio player which can perform playback of not only a DVD-Audio disk but DVD-RAM.

[0039]In this embodiment, although the digital data recorder 300 recorded superdistribution contents on DVD-RAM, it may be recorded on a memory card. In the above superdistributions, the charge amount to the superdistribution contents 10 can be set up at a reasonable price as compared with the retail prices of the sales purpose contents 3. Because, in the retail prices of the sales purpose contents 3. As opposed to various distribution costs concerning circulation of Enhanced-CD, such as a freight cost of Enhanced-CD and DVD-AUDIO, and DVD-AUDIO being added up, Acquisition of the superdistribution contents 10 is because such a distribution cost becomes what is necessary is just to only cancel encryption, and entirely unnecessary.
[0040]As mentioned above, according to this embodiment, even if it is in the situation where the infrastructure for the electronic data distribution represented by the Internet etc. is not fixed, promotion of a related score etc. can sell an interactive music content with the gestalt near electronic music distribution. Although Enhanced-CD and DVD-AUDIO were used in this embodiment as a recording medium which records music, DVD-AUDIO (DVD-AUDIO, disk which had the function of DVD-ROM) of a hybrid type may be used. Although this embodiment explained as what records the container which contains superdistribution contents and a superdistribution header in the recording medium of a sales use, the container which contains superdistribution contents and a superdistribution header in the recording medium distributed freely may be recorded.
[0041]Above, explanation of the data structure of a 1st embodiment recorded on the recording medium of this invention, i.e., superdistribution form, is finished.
(A 2nd embodiment) A 2nd embodiment is related with the digital data recorder 100 which records the data of superdistribution form on a recording medium. The composition of the digital data recorder 100 concerning a 2nd embodiment is shown in drawing 9. The digital data recorder 100 of a 2nd embodiment, It realizes by installing an application program for exclusive use in a general-purpose personal computer, It has the input part 101, the control section 102, the encode part 103, the contents storage 104, the takeoff connection 105, the superdistribution contents encryption section 106, the superdistribution header encryption section 107, the sales purpose contents encryption section 108, the Records Department 109, and the characteristic-data takeoff connection 110, Superdistribution contents are recorded on the recording medium 200 of a sales use. Henceforth, explanation about these components is given.
[0042]Although it supposes henceforth that it is a recording object a music content in this embodiment, it may not be restricted to this and picture image data, alphabetic

data, or the data of such combination may be sufficient. Although the reproduction control script 4 and the still picture data 5 were illustrated by a 1st embodiment as data which should be recorded on the recording medium 200 of a sales use, since it differs from the chief aim of this embodiment, explanation is omitted about the procedure in which these are recorded.

[0043]It is connected with pointing devices, such as a mouse and a keyboard, and the input part 101 receives an operator's directions. Here, with an operator's directions, directions of encoding of a music content or the encoded extraction demand of data is mentioned. The control section 102 interprets the demand of the input part 101, and directs it to the encode part 103 which mentions encoding a music content later. Or it directs to the takeoff connection 105 which mentions too later taking out the music content currently recorded on the contents storage 104 mentioned later.

[0044]The encode part 103 codes the fundamental tone currently recorded on the master tape etc. which are not illustrated to the digital data of for example, LPCM form, compresses it into AAC form, and generates a music content. The content ID 11 shown in a 1st embodiment after that is generated. In the digital data recorder 100, the encode part 103 is not indispensable. When requesting encoding of a music content from an external contractor and recording the encoded data on the contents storage 104, it is because the encode part 103 becomes unnecessary.

[0045]The contents storage 104 is a mass hard disk drive, and stores the music content obtained by encoding of the encode part 103, and the content ID 11 shown in a 1st embodiment. The takeoff connection 105 takes out the content ID 11 shown in the music content and a 1st embodiment which were obtained by encoding from the contents storage 104 based on the directions from the control section 102.

[0046]The superdistribution contents encryption section 106 generates the enciphered content 8 by enciphering the superdistribution contents 10 using the decode key 13 explained by a 1st embodiment. Here, the operator of this digital data recorder 100 can set up the decode key 13 freely. The superdistribution header encryption section 107 obtains the encryption header 7 by combining the terms of purchase 12 of the data of the superdistribution form described by the operator, the content ID 11, and the decode key 13, obtaining the superdistribution header 9, and enciphering this. The generated encryption header 7 is given to the enciphered content 8 which the superdistribution contents encryption section 106 enciphered, and the container 6 is obtained.

[0047]The recording medium 200 for sale of the characteristic-data takeoff connection 110 is DVD-AUDIO, When the sales purpose contents 3 need to be

enciphered based on identification information peculiar to a recording medium, the identification information peculiar to a medium currently beforehand recorded at the time of manufacture of the recording medium 200 of a sales use is taken out, and it outputs to the sales purpose contents encryption section 108. The recording medium 200 for sale is Enhanced-CD, and when the sales purpose contents 3 do not need to be enciphered, extraction does not perform identification information peculiar to a medium.

[0048]The sales purpose contents encryption section 108 enciphers the sales purpose contents 3 based on identification information peculiar to a recording medium, when the recording medium 200 for sale is DVD-AUDIO. The recording medium 200 for sale is Enhanced-CD, and when the sales purpose contents 3 do not need to be enciphered, the sales purpose contents encryption section 108 does not encipher. Since it is indicated by JP,5-257816,A about the art enciphered based on identification information peculiar to a medium, detailed explanation is omitted here.

[0049]The Records Department 109 records the container 6 generated by the superdistribution header encryption section 107 and the sales purpose contents enciphered by the second encryption section 108. The operation is explained using the flow chart which shows the contents of processing of drawing 10 henceforth about the digital data recorder constituted as mentioned above. About the following operations, by the encode part 103, encoding of a fundamental tone shall be completed and two or more music contents shall already have been obtained by the contents storage 104.

[0050]If the control section 102 is started, the control section 102 will wait for selection of what should be recorded on the recording medium 200 of a sales use among two or more contents stored in the contents storage 104 in Step S1. If contents are chosen, in Step S2, the control section 102 will wait the music content from an operator for the recording instruction to the recording medium 200 of a sales use. The recording instruction of the purport that it records for the purpose of sale, and the recording instruction of the purport that it records for the purpose of a superdistribution are one of recording instruction here. When recording instruction occurs, the control section 102 judges the recording instruction of the purport that it records by a sales purpose in Step S3, and the recording instruction in it and superdistribution form.

[0051]When an operator performs recording instruction of the contents of a sales use, in Step S3, it is judged with the recording instruction of the contents of a sales use having been made. In this case, the control section 102 shifts to Step S8 from Step S3,

and judges whether the type of the recording medium 200 of a sales use is DVD-AUDIO, or it is Enhanced-CD in Step S8. If it is Enhanced-CD, it shifts to Step S6 from Step S8, and it points to extraction of the music content and content ID which were chosen as the takeoff connection 105, and the music content and content ID which were taken out are made to record on the recording medium 200 of a sales use. On the other hand, if it is DVD-AUDIO, it shifts to step S9 from Step S8. In step S9, the control section 102 directs extraction of a suitable music content and content ID to the takeoff connection 105, and the taken-out music content is handed over to the sales purpose contents encryption section 108. The sales purpose contents encryption section 108 points to extraction of the peculiar identification information from the recording medium 200 of a sales use to the characteristic-data takeoff connection 110, and the characteristic-data takeoff connection 110 which received this takes out peculiar identification information from the recording medium 200 of a sales use. Then, it shifts to Step S10 from step S9, and the sales purpose contents encryption section 108 enciphers, using the identification information peculiar to a medium taken out by the characteristic-data takeoff connection 110 as an encryption key. Then, it shifts to Step S6 from Step S10, and the Records Department 109 records the sales purpose contents and content ID which were enciphered by the sales purpose contents encryption section 108 on the recording medium 200 of a sales use. Since the recording medium 200 of the sales use was recorded for sales purpose contents by processing from Step S1 to Step S6, operation when the recording instruction of superdistribution contents is made is explained.

[0052]When recording instruction is superdistribution form, the control section 102 makes the takeoff connection 105 take out the selected music content and content ID, and makes it output content ID to the header encryption section 107, and the superdistribution contents encryption section 106 is made to output it to it. The superdistribution contents encryption section 106 generates enciphered content by enciphering the contents taken out in step S4. By making it encipher by the control section 102 combining the content ID 11, the terms of purchase 12, and the decode key 13 with the superdistribution header encryption section 107 in Step S5, The encryption header 7 is made to generate and the container 6 is generated by making the encryption header 7 give the enciphered content 8. Then, it shifts to Step S6 and the generated container 6 is made to record on the recording medium 200 of a sales use. If record to a recording medium is completed, supposing it will ask an operator whether end recording work in Step S7 and will end, the processing in this flow chart will be ended. If it continues, it will shift to Step S1 from Step S7. The inside of one or

more contents which should be recorded on the recording medium 200 of a sales use as mentioned above according to this embodiment, Since this will be chosen as the superdistribution contents 10 and this will be enciphered, if record to the reproduction or other recording media has what has the required payment of a remuneration, while fee collection is not performed, the reproduction about the superdistribution contents 10 or record to other recording media can be prevented.

[0053]The accounting information made to charge a dedicated device when enciphering the superdistribution contents 10 and reproducing or buying the superdistribution contents 10, Since the superdistribution header 9 which contains in a dedicated device the decode key 13 of which encryption of the superdistribution contents 10 is made to cancel after fee collection is given to the superdistribution contents 10, whenever playback of the superdistribution contents 10 or record to other recording media is performed, the concert company can acquire a profit.

[0054]Above, explanation of a 2nd embodiment is finished.

Explanation about the digital data recorder 300 is given as (a 3rd embodiment), next a 3rd embodiment. From the side of acquisition of the superdistribution contents 10, if the internal configuration of the digital data recorder 300 is described functionally, the internal configuration of the digital data recorder 300 is shown in drawing 11. Drawing 11 is a figure showing the internal configuration of the digital data recorder 300 of a 3rd embodiment. Originally, the digital data recorder 300 is a digital data recorder of type corresponding to electronic music distribution, and the download function 313 in electronic music distribution, i.e., the communications department, receives contents from the Internet for counter value, and it has a function recorded on the recording medium 650 of an acquisition use. Since it is the type corresponding to electronic music distribution, the digital data recorder 300 has the communications department for communicating the Internet, and a charging part for settling money on a communication line, when electronic commerce technology is performed in a communication line.

[0055]In drawing 11, the digital data recorder 300 of a 3rd embodiment, It realizes by generally installing an application program for exclusive use in a general-purpose personal computer, The input part 301, the indicator 302, the control section 303, the takeoff connection 304, the superdistribution header decoding section 305, the superdistribution contents decoding section 306, the characteristic-data takeoff connection 307, the superdistribution contents re-encryption section 308, the Records Department 309, the charging part 310, the accounting information storage

312, It has the communications department 313 and the recording rate Management Department 314.

[0056]It is connected with pointing devices, such as a mouse and a keyboard, and the input part 301 receives purchase directions of the music from an operator. With the purchase of the music in a "superdistribution", the act of "recording the data of superdistribution form on another recording medium" is included. Here, the act of a digital output terminal making a digital output a ********** case perform to these digital output terminals at a digital data recorder and digital data playback equipment is also included in "the purchase of music." It is because this recording medium can be made to record the superdistribution contents 10 on it using this drive device if the drive device of another recording medium is connected to such a digital output terminal. In this embodiment, the digital data recorder 100 has a digital output terminal, and has connected the drive device of DVD-RAM via a cable.

[0057]The indicator 302 presents visually the information on the contents of the superdistribution contents 10, the frame of the remuneration at the time of purchasing this, etc. by displaying an interactive screen based on the reproduction control script 4 and the still picture data 5 which are recorded on the recording medium 200 of the sales use. The control section 303 interprets an operator's directions inputted through the input part 301, and directs to other components. Or the next processing is directed according to the result which other components outputted. For example, if there are purchase directions of a related score from an operator, extraction of the superdistribution contents 10 currently recorded on the recording medium 200 of the sales use and the superdistribution header 9 will be directed to the takeoff connection 304 mentioned later.

[0058]The takeoff connection 304 takes out the container 6 currently recorded on the recording medium 200 of the sales use shown in a 2nd embodiment. The superdistribution header decoding section 305 will decrypt using the decode key 13 to the encryption header 7 in the container 6 contained in it, if the takeoff connection 304 takes out the container 6. If the superdistribution header 9 is obtained by decoding, the terms of purchase of the superdistribution contents 10 can be shown to an operator by referring to the content ID 11, the terms of purchase 12, and the decode key 13 which are contained in this. The thing beforehand stored in the application program installed in the digital data recorder 300, for example or the thing distributed from a charging center via a communication line is used for the decode key used when decoding a superdistribution header.

[0059]The superdistribution contents decoding section 306 will decrypt the enciphered content 8 using the decode key 13 contained in this, if the superdistribution header decoding section 305 decrypts the superdistribution header 9. The characteristic-data takeoff connection 307 takes out identification information peculiar to a medium from the recording medium 650 of an acquisition use. Since the recording medium 650 of an acquisition use is DVD-RAM, the information written to BCA (Burst Cutting Area) is used for it as identification information peculiar to a medium here. For every disk, identification information peculiar to this medium is unique, is information moreover recorded usually at the time of disk manufacture, and cannot be rewritten. Therefore, even if an operator with bad faith should reproduce the contents of the disk, since the identification information which becomes a basis of a decode key differs, it cannot decrypt, but it becomes possible to protect the copyright of data certainly.

[0060]The superdistribution contents re-encryption section 308 enciphers the superdistribution contents 10 which the superdistribution contents decoding section 306 decrypted based on identification information peculiar to recording-medium 650 medium of the acquisition use which the characteristic-data takeoff connection 307 took out. The Records Department 309 records the superdistribution contents 10 enciphered by the superdistribution contents re-encryption section 308 on the recording medium 650 of an acquisition use.

[0061]If the charging part 310 has a terminating notice of processing of the Records Department 309, from the terms of purchase 12 acquired when the superdistribution header decoding section 305 decoded the superdistribution header 9, it will compute the charge amount based on the accounting information by reading accounting information, and will include it in accounting information. The accounting information storage 312 is equivalent to the hard disk of a personal computer, and stores the accounting information containing the charge amount which the charging part 310 computed. As for accounting information, since it is necessary to prevent an operator with bad faith altering accounting information here, it is desirable to store in a hard disk in the state where it enciphered, or to store in the secure field (field which cannot be accessed in an operator's normal operation) in a hard disk.

[0062]In suitable timing the accounting information which the communications department 313 comprised a modem device connected to the communication line, and its control software, and was recorded on the accounting information storage 312, and an operator's operator ID, It transmits to the host computer 600 currently installed in the charging center of a music center via a communication line. Here, the time of

reaching constant value with charge amount, the time of reaching on the fixed date, etc. can be considered to be suitable timing. Of course, it is good, though it connects with a host computer whenever an operator records on the recording medium 650 of an acquisition use.

[0063]The recording rate Management Department 314 **********s this recording rate, whenever the Records Department 309 has memorized the recording rate which recorded the same superdistribution contents 10 on the recording medium 650 of the acquisition use and the Records Department 309 records the same superdistribution contents 10 on the recording medium 650 of an acquisition use. Operation of the digital data recorder constituted as mentioned above is explained still in detail using the flow chart which shows the contents of processing of drawing 12 henceforth.

[0064]If loaded with the recording medium 200 of a sales use, the control section 303 will start processing of this flow chart, and will wait to perform operation of the purport that he wishes introduction of a related score in Step S20. If such operation is performed, in Step S21, the takeoff connection 304 will read the reproduction control script 4 and the still picture data 5 from the added value field 2 of the recording medium 200 of the sales use, and the interactive screen shown in drawing 8 will be displayed on the indicator 302. Then, it waits to shift to Step S22 and to perform purchase directions of the superdistribution contents 10 from an operator. When purchase directions are performed, it shifts to Step S23 from Step S22, and the takeoff connection 304 is made to end processing, when an operator performs cancellation operation, but to pick out the container 6 containing the encryption header 7 enciphered from the recording medium 200 of a sales use. Then, in Step S24, the superdistribution header 9 is obtained by decrypting the encryption header 7 in the taken-out container 6. If the superdistribution header 9 is obtained, in Step S25, the same superdistribution contents 10 will read the number of times recorded until now from the recording rate Management Department 314. The number of times of digital output permission is read from the superdistribution header 9 obtained by decoding in Step S26 with it. If the number of times of digital output permission is read, it will set to Step S27 and it will be judged whether the recording rate of until is equal to the number of times of digital output permission. Since the digital output of the superdistribution contents 10 beyond this cannot be permitted if equal, processing is ended as it is. On the other hand, if an old recording rate is less than the number of times of digital output permission, the control section 303 uses the decode key 13 in

the superdistribution header 9 for the superdistribution contents decoding section 306 in Step S28, and makes the enciphered content 8 in a container decrypt.
[0065]When decoding is performed, the control section 303 makes the characteristic-data takeoff connection 307 acquire identification information peculiar to a medium from the recording medium 650 of an acquisition use in Step S29, and makes the superdistribution contents re-encryption section 308 encipher data by using acquired identification information as an encryption key. Then, it shifts to Step S30 and the data enciphered by the Records Department 309 is made to record on the recording medium 650 of an acquisition use.
[0066]When record by the Records Department 309 is completed, the control section 303 makes the charging part 310 compute charge amount based on the purchase-prices information in the terms of purchase 12, and is made to store in the accounting information storage 312 as accounting information in Step S31. If waiting and such timing come, that timing suitable after making accounting information store to transmit accounting information in Step S32 comes, In Step S33, the control section 303 makes the communications department 313 take out the accounting information recorded on the accounting information storage 312, and operator ID, makes it transmit to the host computer 600 in a charging center, and ends processing.
[0067]According to this embodiment, the consumers who acquired the recording medium 200 of the sales use as mentioned above, Only when it has agreed on the purchase in onerousness of these superdistribution contents 10, the superdistribution contents 10 currently recorded on the recording medium 200 of the sales use are recorded on the recording medium 650 of an acquisition use, Since only the accounting information which shows the frame of the remuneration to this record act is made to transmit to a charging center via a communication line, there is no necessity of making the superdistribution contents 10 transmitting to a communication line. Therefore, since the telex rate gold which consumers should pay can be managed with a small sum even if it is in the state which the access speed of a communication line cannot say that it is late and the infrastructure of electronic music distribution is fixed, dealing of the superdistribution contents 10 is cheaply realizable.
[0068]Above, explanation of a 3rd embodiment is finished, and a 4th embodiment is described continuously.
(A 4th embodiment) A 4th embodiment is related with the digital data playback equipment which performs reproduction in the onerousness of superdistribution contents. Although this digital data playback equipment 400 differs in the point which

decrypts the data of the superdistribution form in the recording medium 200 of a sales use as it is, without recording on other recording media, and is reproduced from the digital data recorder 300 explained by a 3rd embodiment greatly, The digital data playback equipment 400 has the download function in electronic music distribution, i.e., the function to receive contents from the Internet for counter value, like the digital data recorder 300 in a 3rd embodiment. Therefore, digital data playback equipment includes many digital data recorders 300 and common components. Drawing 13 is a figure showing the composition of the digital data playback equipment concerning a 4th embodiment. Among the components of the digital data playback equipment in drawing 13, about the digital data recorder 300 and a common component, the same reference mark as the digital data recorder 300 is attached, and explanation is omitted. On the other hand, what attached the reference mark of the level of No. 400 among the components of digital data playback equipment (the regenerating section 401, the reproduction frequency Management Department 402), It is a component peculiar to the digital data playback equipment 400 which the digital data recorder 300 does not possess, and the component of these is explained henceforth.

[0069]The regenerating section 401 in drawing 13 reproduces the superdistribution contents 10 decrypted by the superdistribution contents decoding section 306. A start of reproduction of the superdistribution contents 10 will tell that to the charging part 310. When the regenerating section 401 transmits a reproduction start to the charging part 310 and reproduction of the superdistribution contents 10 is performed in a 4th embodiment, suitable fee collection is made.

[0070]The reproduction frequency Management Department 402 **********s this reproduction frequency, whenever the regenerating section 401 has memorized the reproduction frequency which reproduced the same superdistribution contents 10 and the regenerating section 401 reproduces the same superdistribution contents 10. Operation of the digital data playback equipment constituted as mentioned above is explained still in detail using the flow chart which shows the contents of processing of drawing 14 henceforth.

[0071]In this flow chart, it is the processing as the flow chart which shows the contents of processing of drawing 12 that the step from Step S28 and Step S31 to Step S33 is the same from Step S20 to Step S24. On the other hand, since it is processing that Step S41 to the step S46 is peculiar to a 4th embodiment, only these steps are explained. If the encryption header 7 in the taken-out container 6 is decrypted in Step S24 and the superdistribution header 9 is obtained, In Step S41, the control section 303 of digital data playback equipment reads the number of times by

which the same superdistribution contents 10 were reproduced until now from the reproduction frequency Management Department 402. With it, the number of times of a reproducing permission is read from the superdistribution header 9. Since reproduction of the superdistribution contents 10 beyond this cannot be permitted if the control section 303 judges whether old reproduction frequency is less than the number of times of a reproducing permission and it is equal in Step S42 if the number of times of a reproducing permission is read, processing is ended as it is.

[0072]If old reproduction frequency is less than the number of times of a reproducing permission, a present date will be read in Step S43, and the control section 303 will read reproduction permission time and the reproducing permission date from the superdistribution header 9 in Step S44. If these are read, it will be judged whether in Step S45, the present date has already passed reproduction permission time and the reproducing permission date. If it has not passed, it shifts to Step S28 from Step S45, the decode key 13 in the superdistribution header 9 is used for the superdistribution contents decoding section 306, and the enciphered content 8 in a container is made to end processing, if it has passed, but to decrypt. Then, in Step S46, the regenerating section 401 is controlled to reproduce the superdistribution contents 10.

[0073]Since it transmits that playback began to the charging part 310 as mentioned above at the time of the playback start of the superdistribution contents 10 according to this embodiment, whenever the superdistribution contents 10 are played, the concert company can acquire a profit. The digital data recorder which made the acquisition function of the superdistribution contents 10 in a 3rd embodiment and the regenerative function of the superdistribution contents 10 unify may be constituted.

[0074]Above, explanation of a 4th embodiment is finished. Next, a 5th embodiment is described.

(A 5th embodiment) Although it assumed that a music content was distributed using a recording medium in a 1st embodiment - a 4th embodiment, it assumes that a music content is distributed in broadcast waves, such as not only a recording medium but the Internet, satellite broadcasting, and a cable TV, in a 5th embodiment. Drawing 15 is a figure showing the distribution gestalt of the music content in a 5th embodiment. In this figure, the music content which the contents packaging device 700 created is a figure showing being distributed via DVD-Audio701, CD702, the Internet 703, the cable TV 704, and the communications satellite 705. On the other hand in this figure, the contents playback device 801 - the contents playback device 809 all, It is playback equipment which reproduces a music content, Although it is exclusively for the playback equipment 801 of the high-class machine only for music content

playback, and music content playback, hardware for exclusive use in the playback equipment 802 and 803 of a low-grade machine, the portable playback equipment 804 and 805 only for music content playback, and a general-purpose personal computer. There are the playback equipment 806 and 807 with which it was made to equip, the playback equipment 808 set top box type [for reception of satellite broadcasting or CATV], and 809 grades.

[0075]Some playback equipment used as the distribution destination of a music content is type [various] as mentioned above. The household equipment type playback equipment 801 only for music content playback and 802 grades possess dedicated hardware, in order to cancel encryption. On the other hand, the general-purpose personal computer type playback equipment 806 and 807 grades cancel encryption by not providing such dedicated hardware but operating decoding software on general-purpose hardware. From these things, general-purpose personal computers have not fixed a copyright protection mechanism, and household equipment type playback equipment can be said to be that a copyright protection mechanism is ending with maintenance. The quality of a household equipment at the time of reproducing contents is high, and a general-purpose personal computer has the low quality at the time of reproducing contents. Therefore, as for the playback equipment with the high quality of a recycled article of contents, the copyright protection mechanism is fixed, and, as for the playback equipment with the low quality of a recycled article of contents, it turns out that a copyright protection mechanism has not been fixed.

[0076]If the internal configuration of the contents packaging device 700 and the playback equipment 801-809 is described functionally, it will become like drawing 16. Drawing 16 is a figure showing the internal configuration of the contents packaging device 700 in a 5th embodiment, and the contents playback devices 801-809. In this figure, the contents packaging device 700 contains the contents coding part 706, contents quality and a code conversion table storage 707, the contents encryption section 708, and the contents packing part 709.

[0077]The contents coding part 706 obtains two or more contents from which the quality at the time of reproduction differs by coding the candidate for distribution by a different method. By this coding, the contents 710 for sale and the contents 711 for sample offer reproduced in the low quality in which quality is inferior to the contents for sale shall be obtained. Contents quality and the code conversion table storage 707, The quantifying bit number and sampling frequency at the time of carrying out the numerals of the contents, The 2nd conversion table that made the group the 1st

conversion table matched with the rank which should be given to the contents of this quantifying bit number and a sampling frequency, and the encryption key and cryptographic algorithm which should be used in order to encipher the contents of each rank is stored.

[0078]An example of the 1st conversion table is shown in drawing 17 (a). As shown in drawing 17 (a), for the rank 1 in the 1st conversion table. The quantifying bit number of 24 bits and the sampling frequency of 96 kHz are matched, and for the rank 2. It turns out that the quantifying bit number of 16 bits, the quantifying bit number of 16 bits in the sampling frequency of 44.1 kHz and the rank 3, and the sampling frequency of 22.05 kHz are matched. Thus, the more a quantifying bit number and a sampling frequency are high, the more it turns out that the rank estimator matched is high (here, the rank estimator means that a rank is so high that there are few numerical values).

[0079]An example of the 2nd conversion table is shown in drawing 17 (b). As shown in drawing 17 (b), for the rank 1 in the 2nd conversion table. The encryption key of 1024 bits and an encryption algorithm called RSA are matched, and for the rank 2. It turns out that the encryption key of 512 bits, the encryption key of 56 bits in an encryption algorithm called RSA and the rank 3, and an encryption algorithm called DES are matched. Since safety of RSA is higher than DES among these encryption algorithms, and safety is so high that the bit length of an encryption key is long, the more a rank estimator is high in this way, the more it turns out that the safety of the encryption key matched and an encryption algorithm is high.

[0080]The contents encryption section 708 ranks each contents according to the height of the quality of a recycled article, and enciphers the contents to which the rank was given using the encryption key and encryption algorithm according to the rank shown in the conversion table. The contents 710 for sale obtained by coding of the package are the candidates for distribution, and For example, the quantization frequency of 24 bits, When it has a 96-kHz sampling frequency, the contents encryption section 708 gives the rank estimator of "1" to the contents 710 for sale based on the 1st conversion table shown in drawing 17 (a). After giving a rank estimator, the contents encryption section 708 generates a 1024-bit encryption key (session key) as an encryption key corresponding to the rank 1 with reference to the encryption key column in the 2nd conversion table. Then, with reference to the encryption algorithm column in the 2nd conversion table, the contents encryption section 708 enciphers the encryption key of the 1024-bit length concerned with a public-key-encryption algorithm (RSA), and attaches it to the contents for sale to which the above-mentioned scramble processing was performed.

[0081]On the other hand, the contents 711 for sample offer are the candidates for distribution, and when it has the quantization frequency of 16 bits, and a 44.1-kHz sampling frequency, the contents encryption section 708 gives the rank estimator of "2" to the contents 710 for sale based on the 1st conversion table shown in drawing 17 (a). After giving a rank estimator, the contents encryption section 708 generates a 512-bit encryption key (session key) as an encryption key corresponding to the rank 2 with reference to the encryption key column in the 2nd conversion table. Then, with reference to the encryption algorithm column in the 2nd conversion table, the contents encryption section 708 enciphers the encryption key of the 512-bit length concerned with a public-key-encryption algorithm (RSA), and attaches it to the contents for sample offer to which the above-mentioned scramble processing was performed.

[0082]The contents packing part 709 packs up the contents 710 for sale and the contents 711 for sample offer which were enciphered by the contents encryption section 708, and obtains the package according to a distribution gestalt. When the distribution gestalten of a music content are the Internet, satellite broadcasting, CATV, etc., the contents packing part 709 changes this package into a TCP packet and a transport packet, and outputs it. When the distribution gestalten of a music content are recording media, such as CD-ROM and DVD-ROM, the contents packing part 709 changes a package into the file of forms, such as UDF form (universal disc format), and records it on CD-ROM and DVD-ROM. Thus, if a package is recorded, as shown in drawing 18, the package containing two or more contents will be distributed to various playback equipment. Drawing 18 is a figure showing the package obtained when the contents packing part 709 in a 7th embodiment packed up.

[0083]Then, the contents playback devices 801-809 are explained. As shown in drawing 15, although the contents playback devices 801-809 have a respectively original gestalt, It is common at the point containing the hardware ability and the decoding conversion table storage 810, the hardware ability evaluating part 811, the contents unpacking part 812, the contents decoding section 813, the contents storage 814, and the contents reproduction part 815 which are shown in drawing 16.

[0084]Hardware ability and the decoding conversion table storage 810 store the conversion table which matched a rank estimator, and two or more decode keys and decoding algorithms. Although the rank estimator in the 1st conversion table that contents quality and the code conversion table storage 707 store here, and the 2nd conversion table had a value according to the height of the quality of a recycled article in contents, The rank estimator in the conversion table stored in hardware ability and

the decoding conversion table storage 810 should be careful of being used in order to evaluate the hardware ability which each of the playback equipment 801-808 has. With the hardware ability which each of the playback equipment 801-808 has. In order that the hardware of playback equipment may decode encryption, provide dedicated hardware or no is shown, When the copyright protection mechanism is fixed, it is the value which turned a fixed quantity of the high levels of the release capability of the encryption, It is shown that the copyright protection mechanism is fixed, so that the rank estimator of hardware ability is high, and not having fixed the copyright protection mechanism is shown, so that the rank estimator of hardware ability is low. In this embodiment, the rank estimator for evaluation of hardware ability is expressed using the unit rank estimator A, B, and C, and it is the order of A->B->C and let hardware ability be a high thing. Drawing 17 (c) is a figure showing the hardware ability and the decoding conversion table which hardware ability and the decoding conversion table storage 810 store. Although the rank A in the conversion table of drawing 17 (c) shows that the copyright protection mechanism is fixed, the decode key of 1024 bits and a decryption algorithm called RSA are matched with this rank A. On the other hand, the ranks B and C are the rank estimators which should be given to the playback equipment in which the copyright protection mechanism is not fixed as compared with the playback equipment of the rank A. It turns out that the decode key of 56 bits, the decode key of 56 bits in a decryption algorithm called RSA and the rank C, and a decryption algorithm called DES are matched at rank estimator B.

[0085]By the hardware ability evaluating part's 811 detecting the existence of possession of the dedicated hardware for decoding encryption of contents, and computing the memory scale which can be used for decoding processing in hardware, The rank estimator which shows the performance of the hardware concerned is computed by evaluating the performance of the hardware of playback equipment. If a package is distributed by the contents packaging device 700, the contents unpacking part 812 will acquire this package, and will extract the contents for sale, and the contents for sample offer from this package.

[0086]The contents decoding section 813 chooses the thing according to the rank estimator evaluated by the hardware ability evaluating part 811 among two or more decode keys and the decoding algorithms which can be set to hardware ability and the decoding conversion table storage 810. Only the contents of which encryption should be canceled in a decode key and a decoding algorithm selected among the contents extracted by the contents unpacking part 812 with it are separated, and encryption of the separated contents is canceled.

[0087]When the contents playback device 801 which is high-class apparatus of the household equipment mentioned above here is an object, it is explained how decoding of the contents by the contents decoding section 813 is performed. Since this contents playback device 801 has the hardware for exclusive use for decoding encryption, hardware ability will be estimated the rank A by the hardware ability evaluating part 811. Since the 1024-bit decode key and the decoding algorithm of RSA are matched with the rank A in hardware ability and the decoding conversion table storage 810, the contents decoding section 813 chooses a 1024-bit decode key and the decoding algorithm of RSA. On the other hand, since the contents 710 for sale are enciphered as a 1024-bit enciphering key using the encryption algorithm of RSA, the contents decoding section 813 separates only the contents 710 for sale among the contents which the contents unpacking part 812 extracted from the package. And in order to cancel public key encryption, decoding processing is performed using the decode key distributed beforehand.

[0088]Then, when the wide use personal SOKON pewter type contents playback device 806 of which encryption is canceled by operating decoding software on general-purpose hardware is an object, it is explained how decoding of the contents by the contents decoding section 813 is performed. Since only general-purpose hardware has this contents playback device 806, hardware ability will be estimated the rank C by the hardware ability evaluating part 811. On the other hand, since the 56-bit decode key and the decoding algorithm of DES are matched with the rank C in hardware ability and the decoding conversion table storage 810, the contents decoding section 813 chooses a 56-bit decode key and the decoding algorithm of DES. On the other hand, since the contents 711 for sample offer are enciphered as a 56-bit enciphering key using the encryption algorithm of DES, the contents decoding section 813 separates only the contents 711 for sample offer among the contents which the contents unpacking part 812 extracted from the package. On the other hand, since DES is a common key encryptosystem, it can decode contents with the encryption key used at the time of encryption. Therefore, the contents decoding section 813 picks out an encryption key from the package concerned, and performs decoding processing, using this as a decode key.

[0089]The contents storage 814 stores the contents decoded by the contents decoding section 813. The contents reproduction part 815 reproduces the decoded contents once stored in the contents storing means 723. According to this embodiment, encryption processing of a level which is different, respectively in the contents 710 for sale and the contents 711 for sample offer reproduced in quality

lower than these contents 710 for sale is performed as mentioned above, Since it was made to carry out packaging, by the contents packing means 713, as a package in the reproduction side. When the contents according to the reproduction performance of hardware come to be chosen and reproduced and the playback equipment of the distribution destination of a music content has a general-purpose type, high-class type difference, the contents according to this will be reproduced. Therefore, without taking the reproduction environment of contents into consideration, the side which provides contents can provide simultaneously the contents from which quality differs, and can protect the copyright over contents safely.

[0090]Explanation of a 5th embodiment is finished above. Next, a 6th embodiment is described.

(A 6th embodiment) The contents coding part 706 obtains the contents 711 for sample offer by coding the head part for distribution, and a 6th embodiment. By coding the remaining portion for distribution, the contents 710 for sale are obtained and it is related with improvement of the contents packaging device 700 of packing this up in a package. Drawing 19 is a figure showing the contents packaging device 700 in a 6th embodiment, and the contents playback devices 801-809.

[0091]In this embodiment, the contents encryption section 708 gives a predetermined rank to the contents for sample offer, and gives a higher rank to difference contents. Enciphering the contents to which the rank was given using the encryption key and encryption algorithm according to the rank shown in the conversion table, the contents packing part 709 packs up said two or more enciphered contents, and generates a package. Drawing 20 is a figure showing the package obtained when the contents packing part 709 in a 7th embodiment packed up.

[0092]According to this embodiment, there is an advantage of the size of the package at the time of contents packaging being reduced, and reduction of transmission capacity and a package being recorded as a result, for example, being able to perform capacity saving of recording media, such as a hard disk and CD-ROM, as mentioned above. Although it had explained based on the above-mentioned embodiment, it only showed as an example of a system which can expect the best effect in the actual condition. Change implementation of this invention can be carried out in the range which does not deviate from the gist. As a typical change embodiment, there are some which are shown in (a) - (f) below.

[0093](a) According to a 1st embodiment - a 4th embodiment, the recording medium 650 of an acquisition use may be transposed to hard disks other than an optical disc, semiconductor memory, etc., although explained as optical discs, such as DVD-RAM.

(b) When recording accounting information in the 3rd – a 4th embodiment, it explained considering the accounting information storage 312 as a hard disk of a personal computer, but it is possible for it not to be restricted to a hard disk and to transpose to recording media, such as an IC card.

[0094](c) Although explained supposing comprising a personal computer and being used in a home about the digital data recorder 500 in the 1st – a 4th embodiment, it cannot be overemphasized that it may install in stores, such as the existing record shop.

(d) Although the information which an information provider provides was explained as a music content in the 1st – a 4th embodiment, Of course, what is not restricted to this and a music content, an image content, text, or an image content, a music content and text combined may be used.

[0095](e) In a 5th embodiment, although the contents 710 for sale and the contents 711 for sample offer shall be distributed, it is not restricted to this, and when distributing three or more contents using the contents which have still more gradual quality, it can apply.

(f) A machine program may realize the procedure (drawing 10, drawing 12, drawing 14) etc. which were explained with reference to the flow chart by this embodiment in the 1st – a 6th embodiment, this may be recorded on a recording medium, and it may be made the object of circulation and sale. Although there are an IC card, an optical disc, a floppy disk, etc. in such a recording medium, the machine program recorded on these is appropriated for the use by being installed in a general purpose computer. This general purpose computer executes the installed machine program one by one, and realizes the function of the digital data recorder shown in this embodiment, and digital data playback equipment.

[0096]

[Effect of the Invention]The recording medium applied to this invention as explained above, The 1st contents and the 2nd contents that the 1st contents are different contents and are enciphered based on the 1st cipher system, The 1st key information used in order to be matched with the 2nd contents and to make the encryption in the 2nd contents cancel is included, Since the header enciphered with the 2nd cipher system that is a cipher system with which release of the encryption is performed is recorded only when the 2nd key information beforehand distributed to the predetermined device is used, The 1st contents are a famous artist's newly released pieces of music, and if it is a score in which the 2nd contents are related, the

consumers who purchased these 1st contents can obtain the music content of this related score by canceling encryption of the 1st cipher system and the 2nd cipher system. Since the 2nd key information for release of this encryption to make that encryption canceling should just load with main story recording media the predetermined device distributed beforehand, if consumers have such a predetermined device at the house, they do not need to apply a long time and do not need to download contents. In order to purchase the 2nd contents, it is not necessary to go to the retail store of contents specially. Thus, consumers can obtain simply the score relevant to a famous artist's newly released piece of music.

[0097]Since various distribution costs concerning circulation of a recording medium, such as a freight cost, are added up to this one recording medium, the concert company can set up the charge amount to the 2nd contents at a reasonable price, and consumers can obtain the 2nd contents cheaply. In order to defend here the 2nd contents that should perform reproduction or acquisition for counter value from unjust reproduction and record, When the 2nd contents must be enciphered with algorithms with a heavy processing load and high safety, such as an algorithm of public key use, and the 2nd contents have data size of several megabytes, we are anxious about the time which release of the encryption takes turning into a long time, but. Since the 2nd contents themselves are enciphered with the 1st cipher system and a header is enciphered with the 2nd cipher system, the recording medium concerning this invention can extract the part enciphered with the algorithm of public key use only to a header, when the 2nd cipher system is an algorithm of public key use.

[0098]Thus, since the 1st key information for extracting the part enciphered with an algorithm with high safety only to a header, and canceling encryption of the 1st contents in it is stored, As compared with the case where the 2nd contents themselves are enciphered with the algorithm of public key use, time until it cancels the encryption in the 2nd contents can be shortened. Since time after this points to acquisition and reproduction of superdistribution contents until it becomes acquisition and renewable is short and it ends, those who wished the purchase of superdistribution contents are not irritated for fun, and the probability which cancels purchase becomes low. Since it is thought that the time which this release takes becomes very shorter than the time which download of the music content in electronic music distribution takes, the operator can appreciate immediately the superdistribution contents which wished acquisition or reproduction.

[0099]****** [that said predetermined device has here the function to charge, and said header permits reproduction of the 2nd contents or record to other recording

media further], The use limitation information which shows the upper limit frequency in the case of permitting reproduction or record to other recording media, When record is permitted by reproduction or other recording media of the 2nd contents, the accounting information which shows the fee which record to the fee or other recording media which the reproduction which should be made to charge said predetermined device takes takes is included, and a peach is good.
[0100]It does not permit infinitely that the 2nd contents' being recorded on other recording media, for example and the 2nd contents are reproduced according to this recording medium, Since a maximum can be set up, the duplicate of the 2nd contents can overflow and the 2nd contents can be prevented from reproduction of the 2nd contents being performed frequently and obsoleting. ****** [that said predetermined device has here the function to charge, and said header permits reproduction of the 2nd contents, or record to other recording media further], The permission period information which shows the permission period in the case of permitting record to reproduction or other recording media, When record is permitted by reproduction or other recording media of the 2nd contents, the accounting information which shows the fee which record to the fee or other recording media which the reproduction which should be made to charge said predetermined device takes takes may be included.
[0101]According to this recording medium, since the consent cannot perform the duplicate or reproduction of the 2nd contents, only the period shown in that permission period information can give premium added value, such as available only during this season and a limited time offer, to the 2nd contents. The storing means which stores at least one or more contents which should be recorded on a recording medium here, The selecting means which chooses the contents as superdistribution contents when what should charge record to the reproduction or other recording media exists in said one or more contents, So that the reproduction about selected superdistribution contents or record to other recording media may be prevented, while fee collection is not performed, The 1st encoding means that enciphers superdistribution contents based on the 1st cipher system, The creating means which generates a superdistribution header including the key information of which encryption of superdistribution contents is made to cancel, The generated superdistribution header is enciphered based on the 2nd cipher system whose safety is higher than said 1st cipher system, A digital data recorder provided with the 2nd encoding means given to superdistribution contents and the recording device which will be recorded on a recording medium by using one or more contents as digital data if a superdistribution header is given may be used.

[0102]If record to those reproduction or other recording media has what has the required payment of a remuneration among one or more contents which should be recorded on the recording medium of a sales use according to this digital data recorder, this will be chosen as superdistribution contents, Since this is enciphered, while fee collection is not performed, the reproduction about superdistribution contents or record to other recording media can be prevented.
[0103]The accounting information which enciphers superdistribution contents and shows the remuneration to superdistribution contents, Since the superdistribution header which contains in the playback equipment of superdistribution contents the contents key of which encryption of superdistribution contents is made to cancel is given to superdistribution contents when a remuneration is paid, Whenever playback of superdistribution contents or record to other recording media is performed, the concert company can acquire a profit.
[0104]If the recording medium with which the charger stage which loads with either [at least] the 1st recording medium or the 2nd recording medium here, and the charger stage were loaded is the 1st recording medium, The reading means which reads superdistribution contents from the 1st recording medium, and the presenting means which shows an operator the remuneration to record to the 2nd recording medium of superdistribution contents, The release means of which encryption of the superdistribution contents read from the 1st recording medium is canceled when the operation which the receiving means which receives the operation from an operator, and the receiving means received is operation of the purport that it agrees with the payment of a remuneration, If the charging means charged to an operator and the charger stage are loaded with the 2nd recording medium used as the archive destination of superdistribution contents when directions of the purport that it agrees with the payment of a remuneration are received from an operator, A digital data recorder provided with the recording device recorded on the 2nd recording medium of an archive destination by using as digital data the superdistribution contents of which encryption was canceled may be used.
[0105]According to this digital data recorder, the consumers who acquired the recording medium, Since the superdistribution contents currently recorded on the recording medium are recorded on the recording medium of an acquisition use and fee collection to this record act is performed only when it has agreed on the payment of the remuneration of these superdistribution contents, there is no necessity of making superdistribution contents transmitting to a circuit. Therefore, since the telex rate gold which consumers should pay can be managed with a small sum even if it is in the

state which the access speed of a circuit cannot say that it is late and the infrastructure of electronic music distribution is fixed enough, dealing of superdistribution contents is cheaply realizable.

[0106]The charger stage which loads with a recording medium here, and the reading means which will read this if superdistribution contents are recorded on the recording medium with which the charger stage was loaded, The presenting means which shows an operator the remuneration to reproduction of superdistribution contents, The release means of which encryption of superdistribution contents is canceled when the operation which the receiving means which receives the operation from an operator, and the receiving means received is operation of the purport that it agrees with the payment of a remuneration, When directions of the purport that it agrees with the payment of a remuneration are received from an operator, digital data playback equipment provided with the charging means charged to an operator and the reproduction means which reproduces the superdistribution contents of which encryption was canceled may be used.

[0107]Since it charges at the time of the playback start of superdistribution contents according to this digital data playback equipment, whenever superdistribution contents are played, the concert company can acquire a profit. The encoding means which obtains two or more contents from which the quality at the time of reproduction differs by coding the candidate for distribution by a different method here, A rank means to rank each contents according to the height of the quality of a recycled article, The conversion table storing means which stores the conversion table which made the group two or more ranks, and the encryption key and cryptographic algorithm which should be used in order to encipher the contents of each rank, A contents packaging device provided with the encoding means which enciphers the contents to which the rank was given using the encryption key and encryption algorithm according to the rank shown in the conversion table, and a packing means to generate the package containing said two or more enciphered contents may be used.

[0108]According to this contents packaging device, perform encryption processing of a level which is different, respectively in the contents for sale and the contents for sample offer reproduced in quality lower than these contents for sale, and by a contents packing means. Since it was made to carry out packaging as a package, in the reproduction side. When the contents according to the reproduction performance of hardware come to be chosen and reproduced and various types, such as a general-purpose type and a high-class type, exist in the playback equipment of the distribution destination of a music content, the contents according to this will be

reproduced. Therefore, without taking the reproduction environment of contents into consideration, the side which provides contents can provide simultaneously the contents from which quality differs, and can protect the copyright over contents safely.

[0109]Obtain the contents for sample offer by coding the part for distribution here, and. The encoding means which obtains difference contents by coding the remaining portion for distribution, A rank means to give a predetermined rank to the contents for sample offer, and to give a higher rank to difference contents, Are making into the group two or more ranks, and the encryption key and cryptographic algorithm which should be used in order to encipher the contents of each rank, and in one group. It is matched by the predetermined rank and for another side to construct, The conversion table storing means which stores the conversion table matched with the rank higher than the predetermined rank concerned, A contents packaging device provided with the encoding means which enciphers the contents to which the rank was given using the encryption key and encryption algorithm according to the rank shown in the conversion table, and a packing means to generate the package containing said two or more enciphered contents may be used.

[0110]According to this contents packaging device, the size of the package at the time of carrying out packaging of the contents is reducible, As a result, there is an advantage of reduction of transmission capacity and a package being recorded, for example, being able to perform capacity saving of recording media, such as a hard disk and CD-ROM.

[Translation done.]

* NOTICES *

JPO and INPIT are not responsible for any
damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.**** shows the word which can not be translated.

3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1](a) It is a figure showing the appearance of Enhanced-CD.

(b) It is a figure showing the physical structure of Enhanced-CD.
[Drawing 2](a) It is a figure showing the appearance of DVD-AUDIO.
(b) It is a figure showing the functional format of DVD-AUDIO.
[Drawing 3]It is a figure showing the plastic case for exclusive use which stored the recording medium for sale.
[Drawing 4]It is a figure showing the data structure of the container 6.
[Drawing 5]It is a figure showing an example of the terms of purchase 12.
[Drawing 6]It is a figure showing how the sales purpose contents 3 in this embodiment and the superdistribution contents 10 circulate.
[Drawing 7](a) It is a figure showing the procedure in which superdistribution contents are bought from the recording medium 200 for -(d) sale to the recording medium 650 of an acquisition use.
[Drawing 8]It is a figure showing an example of the interactive screen displayed on the display screen of playback equipment with the reproduction control script 4 and the still picture data 5.
[Drawing 9]It is a figure showing the composition of the digital data recorder 100 concerning a 2nd embodiment.
[Drawing 10]It is a flow chart which shows the contents of processing of the digital data recorder 100 of a 2nd embodiment.
[Drawing 11]It is a figure showing the internal configuration of the digital data recorder 300 of a 3rd embodiment.
[Drawing 12]It is a flow chart which shows the contents of processing of the digital data recorder 300 of a 3rd embodiment.
[Drawing 13]It is a figure showing the internal configuration of the digital data playback equipment 400 of a 4th embodiment.
[Drawing 14]It is a flow chart which shows the contents of processing of the digital data playback equipment 400 of a 4th embodiment.
[Drawing 15]It is a figure showing the distribution gestalt of the music content in a 5th embodiment.
[Drawing 16]It is a figure showing the internal configuration of the contents packaging device 700 in a 5th embodiment, and the contents playback devices 801-809.
[Drawing 17](a) It is a figure showing an example of the 1st conversion table.
(b) It is a figure showing an example of the 2nd conversion table.
(c) It is a figure showing an example of hardware ability and a decoding conversion table.

[Drawing 18]It is a figure showing the package obtained when the contents packing part 709 in a 5th embodiment packed up.
[Drawing 19]It is a figure showing the internal configuration of the contents packaging device 700 in a 6th embodiment, and the contents playback devices 801-809.
[Drawing 20]It is a figure showing the package obtained when the contents packing part 709 in a 6th embodiment packed up.
[Description of Notations]
1 Contents area
2 Added value field
3 Sales purpose contents
4 Reproduction control script
5 Still picture data
6 Container
7 Encryption header
8 Enciphered content
9 Superdistribution header
10 Superdistribution contents
11 Content ID
12 Terms of purchase
13 Decode key
100 Digital data recorder
101 Input part
102 Control section
103 Encode part
104 Contents storage
105 Takeoff connection
106 Superdistribution contents encryption section
107 Superdistribution header encryption section
108 Sales purpose contents encryption section
109 Records Department
110 Characteristic-data takeoff connection
200 The recording medium of a sales use
300 Digital data recorder
301 Input part
302 Indicator
303 Control section

304 Takeoff connection
305 Superdistribution header decoding section
306 Superdistribution contents decoding section
307 Characteristic-data takeoff connection
308 Superdistribution contents re-encryption section
309 Records Department
310 Charging part
312 Accounting information storage
313 Communications department
314 Recording rate Management Department
400 Digital data playback equipment
401 Regenerating section
402 Reproduction frequency Management Department
500 Communication line
600 Host computer
650 The recording medium of an acquisition use
700 Contents packaging device
706 Contents coding part
707 Contents quality and a code conversion table storage
708 Contents encryption section
709 Contents packing part
710 Contents for sale
711 Contents for sample offer
801 - 809 contents-playback device
810 Hardware ability and a decoding conversion table storage
811 Hardware ability evaluating part
812 Contents unpacking part
813 Contents decoding section
814 Contents storage
815 Contents reproduction part

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－196585
（P2000－196585A）
(43)公開日　平成12年７月14日(2000.7.14)

(51)Int.Cl.⁷	識別記号	FI	テーマコード（参考）
Ｈ０４Ｌ　9/14		Ｈ０４Ｌ　9/00	６４１
Ｇ１１Ｂ　19/02	５０１	Ｇ１１Ｂ　19/02	５０１Ｊ
19/04	５０１	19/04	５０１Ｈ
20/10		20/10	Ｈ

審査請求　未請求　請求項の数29　ＯＬ　（全 29 頁）

(21)出願番号　特願平11－287365

(22)出願日　平成11年10月７日(1999.10.7)

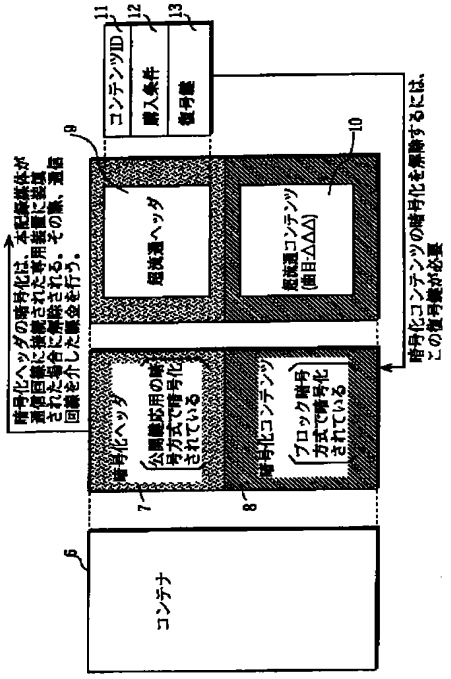
(31)優先権主張番号　特願平10－286177
(32)優先日　平成10年10月８日(1998.10.8)
(33)優先権主張国　日本（ＪＰ）
(31)優先権主張番号　特願平10－297159
(32)優先日　平成10年10月19日(1998.10.19)
(33)優先権主張国　日本（ＪＰ）
(31)優先権主張番号　特願平10－297142
(32)優先日　平成10年10月19日(1998.10.19)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　田川　健二
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　南　賢尚
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100090446
弁理士　中島　司朗　（外１名）

最終頁に続く

(54)【発明の名称】　コンテンツを記録した記録媒体、デジタルデータ記録装置、デジタルデータ再生装置、パッケージを作成するコンテンツパッケージング装置、コンテンツ再生装置、コンピュータ読み取り可能

(57)【要約】
【課題】　電子音楽配信を実現するためのインフラストラクチャが未整備であっても、ある音楽コンテンツを購入した消費者に対して、この音楽コンテンツに関連する音楽コンテンツを低価格で尚且つ手軽に販売することができる記録媒体を提供する。
【解決手段】　記録媒体には、販売目的のコンテンツが記録されており、それと共に、ブロック暗号方式に基づいて暗号化されている超流通コンテンツ１０が記録されている。この超流通コンテンツ１０に付与されている超流通ヘッダ９は、公開鍵応用の暗号化方式に基づいて暗号化されており、ブロック暗号方式の暗号化を解除させる復号鍵１３を含む。この公開鍵応用の暗号方式は、本記録媒体が通信回線に接続された装置３００、４００に装填された場合に、これらの装置により暗号化が解除される暗号方式であり、その暗号化の解除には、通信回線を介した課金が伴う。



1

【特許請求の範囲】

【請求項１】　第１コンテンツと、

第１コンテンツとは異なるコンテンツであって、第１暗号方式に基づいて暗号化されている第２コンテンツと、

第２コンテンツに対応づけられていて、第２コンテンツにおける暗号化を解除させるために用いられる第１鍵情報を含んでおり、所定の装置に予め配布されている第２鍵情報を用いた場合のみ、その暗号化の解除が行われる暗号方式である第２暗号方式にて暗号化されているヘッダとが記録されていることを特徴とする記録媒体。

【請求項２】　前記所定装置は、課金を行う機能を有しており、

前記ヘッダは更に、

第２コンテンツの再生又は他の記録媒体への記録を許諾するか否かと、再生又は他の記録媒体への記録を許諾する場合の上限回数とを示す利用制限情報と、

第２コンテンツの再生又は他の記録媒体に記録が許諾されている場合に、前記所定装置に課金させるべき再生に要する料金又は他の記録媒体への記録に要する料金を示す課金情報とを含むことを特徴とする請求項１記載の記録媒体。

【請求項３】　前記所定装置は、課金を行う機能を有しており、

前記ヘッダは更に、

第２コンテンツの再生又は他の記録媒体への記録を許諾するか否かと、再生又は他の記録媒体に記録を許諾する場合の許可期間を示す許可期間情報と、

第２コンテンツの再生又は他の記録媒体に記録が許諾されている場合に、前記所定装置に課金させるべき再生に要する料金又は他の記録媒体への記録に要する料金を示す課金情報とを含むことを特徴とする請求項１記載の記録媒体。

【請求項４】　前記第１コンテンツは、

記録媒体固有の識別情報を用いて、暗号化されていることを特徴とする請求項１記載の記録媒体。

【請求項５】　コンテンツを含むデジタルデータを記録媒体に記録するデジタルデータ記録装置であって、

記録媒体に記録すべきコンテンツを少なくとも1つ以上格納する格納手段と、

その再生又は他の記録媒体への記録に課金を行うべきものが前記1つ以上のコンテンツに存在する場合、そのコンテンツを超流通コンテンツとして選択する選択手段と、

課金が行われていない間、選択された超流通コンテンツについての再生又は他の記録媒体への記録を防止するよう、第１暗号方式に基づいて超流通コンテンツを暗号化する第１暗号化手段と、

超流通コンテンツの暗号化を解除させる鍵情報を含む超流通ヘッダを生成する生成手段と、

生成された超流通ヘッダを、前記第１暗号方式より安全

2

性が高い第２暗号方式に基づいて暗号化して、超流通コンテンツに付与する第２暗号化手段と、

超流通ヘッダが付与されると、1つ以上のコンテンツをデジタルデータとして記録媒体に記録する記録手段とを備えることを特徴とするデジタルデータ記録装置。

【請求項６】　前記デジタルデータ記録装置は更に記録媒体固有の識別情報を記録媒体から取り出す取出手段と、

超流通コンテンツ以外のコンテンツについては、取出手段により取り出された識別情報を用いて暗号化する第３暗号化手段とを備えることを特徴とする請求項５記載のデジタルデータ記録装置。

【請求項７】　他の記録媒体への記録に課金が必要であり、課金が行われていない間に他の記録媒体に記録されることを防止するため暗号化されているコンテンツである超流通コンテンツを第１記録媒体から読み出して、第２記録媒体に記録するデジタルデータ記録装置であって、

第１記録媒体及び第２記録媒体の少なくとも一方を装填する装填手段と、

装填手段に装填された記録媒体が第１記録媒体であれば、超流通コンテンツを第１記録媒体から読み出す読出手段と、

超流通コンテンツの第２記録媒体への記録に対する対価を操作者に提示する提示手段と、

操作者からの操作を受け付ける受付手段と、

受付手段が受け付けた操作が、対価の支払いに同意する旨の操作である場合、第１記録媒体から読み出された超流通コンテンツの暗号化を解除する解除手段と、

対価の支払いに同意する旨の指示を操作者から受け付けた場合、操作者に対して課金を行う課金手段と、

装填手段に超流通コンテンツの記録先となる第２記録媒体が装填されれば、暗号化が解除された超流通コンテンツをデジタルデータとして記録先の第２記録媒体に記録する記録手段とを備えることを特徴とするデジタルデータ記録装置。

【請求項８】　前記デジタルデータ記録装置は更に装填手段に超流通コンテンツの記録先となる第２記録媒体が装填されれば、記録媒体固有の識別情報を、記録先となる第２記録媒体から取り出す取出手段と、

解除手段により暗号化が解除された超流通コンテンツを、取出手段が取り出した識別情報を暗号鍵として用いて、再度暗号化する再暗号化手段とを備え、

前記記録手段は、

再暗号化手段により再度暗号化された超流通コンテンツを記録先の第２記録媒体に記録することを特徴とする請求項７記載のデジタルデータ記録装置。

【請求項９】　その再生に課金が必要であり、課金が行われていない間の再生を防止するため暗号化されているコンテンツである超流通コンテンツを再生するデジタル

データ再生装置であって、
記録媒体を装填する装填手段と、
装填手段に装填された記録媒体に超流通コンテンツが記録されていればこれを読み出す読出手段と、
超流通コンテンツの再生に対する対価を操作者に提示する提示手段と、
操作者からの操作を受け付ける受付手段と、
受付手段が受け付けた操作が、対価の支払いに同意する旨の操作である場合、超流通コンテンツの暗号化を解除する解除手段と、
対価の支払いに同意する旨の指示を操作者から受け付けた場合、操作者に対して課金を行う課金手段と、
暗号化が解除された超流通コンテンツを再生する再生手段とを備えることを特徴とするデジタルデータ再生装置。

【請求項１０】　複数のコンテンツを含むパッケージを作成するコンテンツパッケージング装置であって、
配布対象を異なる方式にて符号化することにより、再生時の品質が異なるコンテンツを複数得る符号化手段と、
再生品質の高低に応じて、各コンテンツをランク付けするランク付け手段と、
複数のランクと、各ランクのコンテンツを暗号化するために用いるべき暗号鍵及び暗号アルゴリズムとを組にした対応表を格納する対応表格納手段と、
ランクが付与されたコンテンツを、対応表に示されているランクに応じた暗号鍵及び暗号化アルゴリズムを用いて暗号化する暗号化手段と、
前記暗号化された複数のコンテンツを含むパッケージを生成する梱包手段とを備えることを特徴とするコンテンツパッケージング装置。

【請求項１１】　前記対応表格納手段は、
前記高い品質で再生されるコンテンツには安全性が高い暗号が用いられるように、前記ランク情報と暗号鍵および暗号アルゴリズムを組にして格納していることを特徴とする請求項１０記載のコンテンツパッケージング装置。

【請求項１２】　複数のコンテンツを含むパッケージを作成するコンテンツパッケージング装置であって、
配布対象の一部分を符号化することにより試供用コンテンツを得ると共に、配布対象の残りの部分を符号化することにより差分コンテンツを得る符号化手段と、
試供用コンテンツに所定のランクを付与し、差分コンテンツに、より高いランクを付与するランク付け手段と、
複数のランクと、各ランクのコンテンツを暗号化するために用いるべき暗号鍵及び暗号アルゴリズムとを組にしており、一方の組には、所定のランクが対応づけられ、他方の組みには、当該所定のランクより高いランクに対応づけられている対応表を格納している対応表格納手段と、
ランクが付与されたコンテンツを、対応表に示されているランクに応じた暗号鍵及び暗号化アルゴリズムを用いて暗号化する暗号化手段と、
前記暗号化された複数のコンテンツを含むパッケージを生成する梱包手段とを備えることを特徴とするコンテンツパッケージング装置。

【請求項１３】　パッケージからコンテンツを取り出して再生するコンテンツ再生装置であって、
再生装置のハードウェアの性能を評価して、当該ハードウェアの性能を示すランク値を算出する評価手段と、
複数のランク値と、各ランク値に対応する性能を有するハードウェアが暗号化解除処理を行う際、その暗号化解除処理に用いるべき復号鍵及び復号アルゴリズムの組みとを対応づけた対応表を格納している対応表格納手段と、
それぞれが暗号化がなされたコンテンツを複数含むパッケージを装置外部から取得する取得手段と、
対応表における複数の復号鍵及び復号アルゴリズムのうち、評価手段により評価されたランク値に応じたものを選択すると共に、この復号鍵及び復号アルゴリズムにて暗号化が解除されるべきコンテンツをパッケージから取り出して、取り出されたコンテンツの暗号化を解除する解除手段とを備えることを特徴とするコンテンツ再生装置。

【請求項１４】　配布対象の一部分を符号化することにより得られた試供用コンテンツと、配布対象の残りの部分を符号化して、試供用コンテンツより安全性が高い暗号鍵及び暗号アルゴリズムにて暗号化することにより得られた差分コンテンツとを含むパッケージからコンテンツを取り出して再生するコンテンツ再生装置であって、
再生装置のハードウェアの性能を評価して、当該ハードウェアの性能を示すランク値を算出する評価手段と、
試供用コンテンツの暗号化を解除することができる復号鍵及び復号アルゴリズムを低いランク値と対応づけており、差分コンテンツの暗号化を解除することができる復号鍵及び復号アルゴリズムを高いランク値と対応づけた対応表を格納している対応表格納手段と、
それぞれが暗号化がなされたコンテンツを複数含むパッケージを装置外部から取得する取得手段と、
対応表における複数の復号鍵及び復号アルゴリズムのうち、評価手段により評価されたランク値に対応したものを選択すると共に、取得したパッケージから、試供用コンテンツ及び差分コンテンツの何れか一方を取り出して、取り出されたコンテンツの暗号化を解除する解除手段とを備えることを特徴とするコンテンツ再生装置。

【請求項１５】　所定の暗号鍵及び所定の暗号化アルゴリズムにて暗号化された試供用コンテンツと、
試供用コンテンツより高い品質で再生され、前記所定の暗号鍵及び前記所定の暗号化アルゴリズムより安全性がより高い暗号鍵及び暗号化アルゴリズムにて暗号化された販売用コンテンツとが記録されていることを特徴とす

る記録媒体。

【請求項１６】　配布対象の一部分を符号化した後、所定の暗号鍵及び所定の暗号化アルゴリズムにて暗号化することにより得られた試供用コンテンツと、
配布対象の残りの部分を符号化した後、前記所定の暗号鍵及び前記所定の暗号化アルゴリズムより安全性がより高い暗号鍵及び暗号化アルゴリズムにて暗号化することにより差分コンテンツとが記録されていることを特徴とする記録媒体。

【請求項１７】　複数のコンテンツを含むパッケージを作成するコンテンツパッケージング装置と、パッケージからコンテンツを取り出して再生するコンテンツ再生装置とからなるシステムであって、
前記コンテンツパッケージング装置は、
配布対象を異なる方式にて符号化することにより、再生時の品質が異なるコンテンツを複数得る符号化手段と、
再生品質の高低に応じて、各コンテンツをランク付けするランク付け手段と、
複数のランクと、各ランクのコンテンツを暗号化するために用いるべき暗号鍵及び暗号アルゴリズムとを組にした対応表を格納しており、一方の組には、所定のランクが対応づけられ、他方の組みには、当該所定のランクより高いランクに対応づけられている対応表を格納する第１対応表格納手段と、
ランクが付与されたコンテンツを、対応表に示されているランクに応じた暗号鍵及び暗号化アルゴリズムを用いて暗号化する暗号化手段と、
前記暗号化された複数のコンテンツを含むパッケージを生成する梱包手段とを備え、
前記コンテンツ再生装置は、
再生装置のハードウェアの性能を評価して、当該ハードウェアの性能を示すランク値を算出する評価手段と、
複数のランク値と、各ランク値に対応する性能を有するハードウェアが暗号化解除処理を行う際、その暗号化解除処理に用いるべき復号鍵及び復号アルゴリズムとを対応づけた対応表を格納している第２対応表格納手段と、
それぞれが暗号化がなされたコンテンツを複数含むパッケージを装置外部から取得する取得手段と、
対応表における複数の復号鍵及び復号アルゴリズムのうち、評価手段により評価されたランク値に応じたものを選択すると共に、この復号鍵及び復号アルゴリズムにて暗号化が解除されるべきコンテンツをパッケージから取り出して、取り出されたコンテンツの暗号化を解除する解除手段とを備えることを特徴とするシステム。

【請求項１８】　コンテンツを少なくとも1つ以上格納する格納部を有したコンピュータが、読み取ることができる記録媒体であって、
その再生又は他の記録媒体への記録に課金を行うべきものが前記1つ以上のコンテンツに存在する場合、そのコンテンツを超流通コンテンツとして選択する選択ステップと、
課金が行われていない間、選択された超流通コンテンツについての再生又は他の記録媒体への記録を防止するよう、第１暗号方式に基づいて超流通コンテンツを暗号化する第１暗号化ステップと、
超流通コンテンツの暗号化を解除させる鍵情報を含む超流通ヘッダを生成する生成ステップと、
生成された超流通ヘッダを、前記第１暗号方式より安全性が高い第２暗号方式に基づいて暗号化して、超流通コンテンツに付与する第２暗号化ステップと、超流通ヘッダが付与されると、1つ以上のコンテンツをデジタルデータとして記録媒体に記録する記録ステップとからなる手順をコンピュータに行わせる記録プログラムが記録されていることを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項１９】　第１記録媒体、及び、第２記録媒体の何れか一方を装填する装填部を有したコンピュータが読み取ることができる記録媒体であって、
課金が行われていない間に他の記録媒体に記録されることを防止するため暗号化されていている超流通コンテンツが記録された第１記録媒体が、装填部に装填されればこれを第１記録媒体から読み出す読出ステップと、
超流通コンテンツの第２記録媒体への記録に対する対価を操作者に提示する提示ステップと、
操作者からの操作を受け付ける受付ステップと、
受付ステップが受け付けた操作が、対価の支払いに同意する旨の操作である場合、第１記録媒体から読み出された超流通コンテンツの暗号化を解除する解除ステップと、
対価の支払いに同意する旨の指示を操作者から受け付けた場合、操作者に対して課金を行う課金ステップと、
装填部に超流通コンテンツの記録先となる第２記録媒体が装填されれば、暗号化が解除された超流通コンテンツをデジタルデータとして記録先の第２記録媒体に記録する記録ステップとからなる手順をコンピュータに行わせる記録プログラムが記録されていることを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項２０】　記録媒体を装填する装填部を有したコンピュータが読み取ることができる記録媒体であって、
その再生に課金が必要であり、課金が行われていない間の再生を防止するため暗号化されていてる超流通コンテンツが記録された記録媒体が装填部に装填されれば、超流通コンテンツを読み出す読出ステップと、
超流通コンテンツの再生に対する対価を操作者に提示する提示ステップと、操作者からの操作を受け付ける受付ステップと、
受付ステップが受け付けた操作が、対価の支払いに同意する旨の操作である場合、超流通コンテンツの暗号化を解除する解除ステップと、
対価の支払いに同意する旨の指示を操作者から受け付け

た場合、操作者に対して課金を行う課金ステップと、
操作者に対して課金が行われると、暗号化が解除された超流通コンテンツを再生する再生ステップとからなる手順をコンピュータに行わせる再生プログラムが記録されていることを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項２１】　複数のランクと、各ランクのコンテンツを暗号化するために用いるべき暗号鍵及び暗号アルゴリズムとを組にした対応表を格納している対応表格納部を有したコンピュータが読み取ることができる記録媒体であって、
配布対象を異なる方式にて符号化することにより、再生時の品質が異なるコンテンツを複数得る符号化ステップと、
再生品質の高低に応じて、各コンテンツをランク付けするランク付とけステップと、
ランクが付与されたコンテンツを、対応表に示されているランクに応じた暗号鍵及び暗号化アルゴリズムを用いて暗号化する暗号化ステップと、
前記暗号化された複数のコンテンツを含むパッケージを生成する梱包ステップとからなる手順をコンピュータに行わせるパッケージングプログラムが記録されていることを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項２２】　複数のランクと、各ランクのコンテンツを暗号化するために用いるべき暗号鍵及び暗号アルゴリズムとを組にした対応表を格納する格納部を有したコンピュータが読み取ることができる記録媒体であって、
配布対象の一部分を符号化することにより試供用コンテンツを得ると共に、配布対象の残りの部分を符号化することにより差分コンテンツを得る前記符号化ステップと、
試供用コンテンツに所定のランクを付与し、差分コンテンツに、より高いランクを付与するランク付けステップと、
ランクが付与されたコンテンツを、対応表に示されているランクに応じた暗号鍵及び暗号化アルゴリズムを用いて暗号化する暗号化ステップと、
前記暗号化された複数のコンテンツを含むパッケージを生成する梱包ステップとからなる手順をコンピュータに行わせるパッケージングプログラムが記録されていることを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項２３】　複数のランク値と、各ランク値に対応する性能を有するハードウェアが暗号化解除処理を行う際、その暗号化解除処理に用いるべき復号鍵及び復号アルゴリズムとを対応づけた対応表を格納している格納部を有するコンピュータが読み取ることができる記録媒体であって、
コンピュータのハードウェアの性能を評価して、当該ハードウェアの性能を示すランク値を算出する評価ステップと、
それぞれが暗号化がなされたコンテンツを複数含むパッケージをコンピュータ外部から取得する取得ステップと、
対応表における複数の復号鍵及び復号アルゴリズムのうち、評価ステップにより評価されたランク値に応じたものを選択すると共に、この復号鍵及び復号アルゴリズムにて暗号化が解除されるべきコンテンツをパッケージから取り出して、取り出されたコンテンツの暗号化を解除する解除ステップとからなる手順をコンピュータに行わせるパッケージングプログラムが記録されていることを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項２４】　記録媒体に記録すべきコンテンツを少なくとも1つ以上格納する格納部を有したコンピュータが、コンテンツを含むデジタルデータを記録媒体に記録する記録方法であって、
その再生又は他の記録媒体への記録に課金を行うべきものが前記1つ以上のコンテンツに存在する場合、そのコンテンツを超流通コンテンツとして選択する選択ステップと、
課金が行われていない間、選択された超流通コンテンツについての再生又は他の記録媒体への記録を防止するよう、第１暗号方式に基づいて超流通コンテンツを暗号化する第１暗号化ステップと、
超流通コンテンツの暗号化を解除させる鍵情報を含む超流通ヘッダを生成する生成ステップと、
生成された超流通ヘッダを、前記第１暗号方式より安全性が高い第２暗号方式に基づいて暗号化して、超流通コンテンツに付与する第２暗号化ステップと、超流通ヘッダが付与されると、1つ以上のコンテンツをデジタルデータとして記録媒体に記録する記録ステップとからなる手順をコンピュータに行わせることを特徴とする記録方法。

【請求項２５】　前記記録方法は、第１記録媒体及び第２記録媒体の何れかを装填する装填部を有したコンピュータに適用され、第１記録媒体に記録された超流通コンテンツを含むデジタルデータを第２記録媒体に記録する記録方法であって、第２記録媒体への記録に課金が必要であり、課金が行われていない間に第２記録媒体に記録されることを防止するため暗号化されている超流通コンテンツが記録された第１記録媒体が装填部に装填されればこれを第１記録媒体から読み出す読出ステップと、
超流通コンテンツの第２記録媒体への記録に対する対価を操作者に提示する提示ステップと、
操作者からの操作を受け付ける受付ステップと、
受付ステップが受け付けた操作が、対価の支払いに同意する旨の操作である場合、第１記録媒体から読み出された超流通コンテンツの暗号化を解除する解除ステップと、
対価の支払いに同意する旨の指示を操作者から受け付けた場合、操作者に対して課金を行う課金ステップと、

装填部に超流通コンテンツの記録先となる第２記録媒体が装填されれば、暗号化が解除された超流通コンテンツをデジタルデータとして記録先の第２記録媒体に記録する記録手段とからなる手順をコンピュータに行わせることを特徴とする記録方法。

【請求項２６】　記録媒体を装填する装填部を有したコンピュータに適用され、記録媒体に記録されているデジタルデータを再生する再生方法であって、

装填部に装填された記録媒体に、その再生に課金が必要であり、課金が行われていない間の再生を防止するため暗号化されている超流通コンテンツが記録されていればこれを読み出す読出ステップと、

超流通コンテンツの再生に対する対価を操作者に提示する提示ステップと、操作者からの操作を受け付ける受付ステップと、

受付ステップが受け付けた操作が、対価の支払いに同意する旨の操作である場合、超流通コンテンツの暗号化を解除する解除ステップと、

対価の支払いに同意する旨の指示を操作者から受け付けた場合、操作者に対して課金を行う課金ステップと、

操作者に対して課金が行われると、暗号化が解除された超流通コンテンツを再する再生ステップとからなる手順をコンピュータに行わせることを特徴とする再生方法。

【請求項２７】　複数のランクと、各ランクのコンテンツを暗号化するために用いるべき暗号鍵及び暗号アルゴリズムとを組にした対応表を格納している対応表格納部を有したコンピュータに適用され、複数のコンテンツを含むパッケージを作成するコンテンツパッケージング方法であって、

配布対象を異なる方式にて符号化することにより、再生時の品質が異なるコンテンツを複数得る符号化ステップと、

再生品質の高低に応じて、各コンテンツをランク付けするランク付とけステップと、

ランクが付与されたコンテンツを、対応表に示されているランクに応じた暗号鍵及び暗号化アルゴリズムを用いて暗号化する暗号化ステップと、

前記暗号化された複数のコンテンツを含むパッケージを生成する梱包ステップとからなる手順をコンピュータに行わせることを特徴とするコンテンツパッケージング方法。

【請求項２８】　複数のランクと、各ランクのコンテンツを暗号化するために用いるべき暗号鍵及び暗号アルゴリズムとを組にした対応表を格納する格納部を有したコンピュータに適用され、複数のコンテンツを含むパッケージを作成するコンテンツパッケージング方法であって、

配布対象の一部分を符号化することにより試供用コンテンツを得ると共に、配布対象の残りの部分を符号化することにより差分コンテンツを得る前記符号化ステップと、

試供用コンテンツに所定のランクを付与し、差分コンテンツに、より高いランクを付与するランク付とけステップと、

ランクが付与されたコンテンツを、対応表に示されているランクに応じた暗号鍵及び暗号化アルゴリズムを用いて暗号化する暗号化ステップと、

前記暗号化された複数のコンテンツを含むパッケージを生成する梱包ステップとからなる手順をコンピュータに行わせることを特徴とするコンテンツパッケージング方法。

【請求項２９】　複数のランク値と、各ランク値に対応する性能を有するハードウェアが暗号化解除処理を行う際、その暗号化解除処理に用いるべき復号鍵及び復号アルゴリズムとを対応づけた対応表を格納部を有したコンピュータに適用され、パッケージからコンテンツを取り出して再生するコンテンツ再生方法であって、

コンピュータのハードウェアの性能を評価して、当該ハードウェアの性能を示すランク値を算出する評価ステップと、

それぞれが暗号化がなされたコンテンツを複数含むパッケージをコンピュータ外部から取得する取得ステップと、

対応表における複数の復号鍵及び復号アルゴリズムのうち、評価ステップにより評価されたランク値に応じたものを選択すると共に、この復号鍵及び復号アルゴリズムにて暗号化が解除されるべきコンテンツをパッケージから取り出して、取り出されたコンテンツの暗号化を解除する解除ステップとからなる手順をコンピュータに行わせることを特徴とする再生方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、デジタル化された音楽著作物を初めとするコンテンツを記録した記録媒体、コンテンツを記録媒体に記録する装置、記録媒体に記録されているコンテンツを再生する装置、複数のコンテンツをパッケージングする装置、コンピュータ読み取り可能な記録媒体、記録方法、再生方法、パッケージング方法に関する。

【０００２】

【従来の技術】（第１従来技術）次世代の音楽著作物の販売形態がどうあるべきかが、大手音楽会社、音響機器メーカ、有識者の間で盛んに議論されている。現状の音楽著作物の販売形態とは、ポップス、ロック、クラシック等様々なジャンルの音楽著作物をCD、磁気テープ等の記録媒体に記録して販売するという形態であり、このように販売された記録媒体を購入して音楽著作物を鑑賞するというライフスタイルは世界中に浸透しているといえる。

【０００３】記録媒体を用いた販売形態に対抗する販売

形態として、多くの注目を集めているのは、電子音楽配信と呼ばれる販売形態である。電子音楽配信とは、音楽コンテンツ（コンテンツとは、デジタル化された著作物のことをいい、音楽コンテンツとは、特に、デジタル化された音楽著作物のことをいう）の有料配布を、近年、急速な普及を見せているインターネット上で行うものである。この電子音楽配信の特色は、音楽コンテンツの販売の申し出や、音楽コンテンツを購入した者に対しての課金が電子商取引（Electronic Commerce)に準じて行われる点である。即ち、この電子音楽配信において音楽会社は、自身が開設したホームページに様々なコンテンツを紹介しており、消費者は、各音楽会社のホームページをアクセスすることにより、様々なコンテンツを検索することができる。好みのコンテンツがあった場合、消費者はコンテンツの購入要求、操作者ID等を、この音楽会社に通知する。音楽会社は、予め操作者により通知されているクレジットカードの番号に対応する銀行口座に基づいて、コンテンツの購入代金の決済を行うことができる。このような決済後、消費者は、消費者が所有しているコンピュータにコンテンツをダウンロードし、自分の好みのコンテンツを入手することができる。

【０００４】このように電子音楽配信では、対話的な選択操作に応じてダウンロードを行うので、例えば、認知度が高い新譜のコンテンツの販売を行っているホームページにおいて、その新譜のコンテンツを作詞･作曲したアーティストの他の楽譜のコンテンツや、その新譜のコンテンツを歌う歌手の他の楽譜のコンテンツを紹介すれば、これら他の楽譜を消費者に売り込むことができる。即ち、あるアーティストの新譜を購入しようとする消費者は、そのアーティストの関連する楽譜に強い興味を示していることが統計的に明らかであり、電子音楽配信では、そのような関連する複数の楽譜の売り込みを効率的に行うことができるのである。

【０００５】（第２従来技術）第１従来技術で述べたように、音楽コンテンツの配布形態には、記録媒体を用いた販売形態、インターネット等の通信回線を用いた販売形態を初め様々なものがある。記録媒体と一言でいっても、記録媒体には、DVD-Audio、CD等の種類があり、これらは何れも異なった符号化方式により符号化された状態で音楽コンテンツを記録している。また、このような販売形態以外にも、衛星放送やケーブルTV等の放送波にて放送されることにより音楽コンテンツが配布される機会も多い。これらの配布は有償で行われるのが原則であるが、音楽コンテンツの知名度を高める目的で無償で試供される場合もある。

【０００６】記録媒体、放送波、通信回線というように、様々な形態で音楽著作物が配布される場合、たとえ配布すべき音楽著作物が一種類のみであっても、音楽著作物を配布する側は、それぞれの配布形態に応じた形態の音楽コンテンツを作成して配布せねばならない。ここで、異なる符号化方式で符号化せねばならないのは以下の理由による。即ち、既に各世帯に普及している再生装置、及び、これから普及しつつある再生装置には、著作権保護機構の有無や、暗号鍵の安全性の高低、再生時における音楽コンテンツの再生品質の高低が、再生装置毎に異なるので、音楽コンテンツを同一の符号化方式にて一律に送信しても、著作権保護機構が全く活用されなかったり、再生装置が本来備えている再生能力が発揮できない恐れがあるからである。

【０００７】著作権保護機構が既に整備されている再生装置が存在するのなら、全ての形態で配布される音楽コンテンツを安全性が高い暗号鍵にて暗号化しておけば良いように思える。しかし音楽コンテンツには、試供用等、知名度向上の目的で配布されるものがあり、このような音楽コンテンツは低い品質で再生されれば良いので、そのように、低い品質でしか再生されない音楽コンテンツも一律に安全性が高い暗号鍵にて暗号化すれば、試供用に低い品質のコンテンツを再生するにも、そのような安全性が高い暗号鍵による暗号化を解かねばならない。これでは、安全性が高い暗号化を解除するだけの復号能力を有していない再生装置は、試供用のコンテンツを再生することが不可能となり、試供用コンテンツが再生される機会が少なくなってしまう。このように試供用コンテンツが再生される機会が少なくなれば、音楽コンテンツの試供にて、幅広く販売促進を図るという広告活動が本来の目標を失うことになる。以上の理由で、それぞれの配布形態に応じた形態の音楽コンテンツを作成して配布することが、必然的に行われていた。

【０００８】

【発明が解決しようとする課題】ところで第１従来技術において問題となるのは、電子音楽配信を実現するためのインフラストラクチャは、現状、充分整備されているとはいえず、消費者が電子音楽配信にて音楽コンテンツを入手するには、消費者に様々な負担が課されるという点である。ここで電子音楽配信の実現のために不可欠とされているインフラストラクチャのうち、代表的なものは、数メガバイトというデータサイズを有する音楽コンテンツを短時間で伝送することができる高速回線であるが、一般のインターネットユーザは、公衆回線を介してサーバをアクセスを行うことにより、インターネットを利用している。一般のインターネットユーザが利用する公衆回線の伝送速度は、高速回線の伝送速度を大きく下回ることが一般的である。このように一般のインターネットユーザが低速な公衆回線を介して、上述のように複数コンテンツを同時にダウンロードする場合、通信時間が長時間となるので、消費者は、多大な通信料金を通信会社に支払うことになる。極端な場合、コンテンツの購入に関し消費者が音楽会社に支払う料金よりも、通信料金のほうが高くなってしまうことが有り得る。このように、消費者に多大な料金が課されるのであれば、電子音

楽配信を利用しようとする消費者の意欲は消沈してしまう。この料金面の問題にも増して懸念されるのは、複数のコンテンツを送信する場合、公衆回線における転送に要する時間が極めて長くなるので、コンテンツの購入を希望した者を悪戯に苛立たせてしまう点である。このようにコンテンツの転送が長ければ、コンテンツの購入を希望した者は複数コンテンツのダウンロードの途中で、コンテンツの購入をキャンセルしてしまう可能性がある。

【０００９】かといって、記録媒体を用いた販売形態において、電子音楽配信と同様、関連する楽譜のコンテンツを売り込もうとする場合、記録媒体を収納したケースに同梱されるジャケットに、そのような関連する楽譜についてセールスポイントや、販売価格等を印刷しておき、関連楽譜の購入を推薦するという古典的な手法をとらざるを得ない。消費者は、このようなジャケットの印刷内容を見て、関連楽譜に興味を持った場合、その関連楽譜を購入するためコンテンツの小売り店に出向き、その関連楽譜が記録された記録媒体を購入することにより、関連楽譜を入手するのである。

【００１０】ここで小売り店に販売されている記録媒体の小売り価格には、記録媒体の製造や流通に係る様々なコストが計上されている。そのため、新譜が記録された記録媒体、関連楽譜が記録された記録媒体の双方を購入しようとする場合、それら記録媒体の製造や流通に係る様々なコストが計上された小売り価格を、2つのコンテンツのそれぞれについて支払う必要があるので、割高な料金を消費者は支払うことになる。

【００１１】また、現状の記録媒体を用いた販売形態において、消費者が関連楽譜を入手するには、消費者自身がわざわざ記録媒体の小売り店に出向かねばならないので、消費者は気軽に関連楽譜を購入することはできず、記録媒体の小売り店に出向くまでにそのような関連楽譜を購入しようとする意欲を失ってしまうこともある。また第２の従来技術において、音楽コンテンツの供給者は、配布形態に応じて、異なる符号化方式で符号化を行う必要があるので、符号化されるコンテンツの数が多ければ多い程、音楽コンテンツの供給者は、それら音楽コンテンツの管理及び配布に多大なストレスを感じるという点である。このようにストレスを感じるのは、符号化されるコンテンツの数が多くなれば、例えば、販売用のコンテンツと、試供用のコンテンツとを誤って配布する等、誤配布の確率も高くなるからである。このような誤配布が生じれば、販売用コンテンツが公共の場に流出することになり、それらの全てを回収せねば、音楽コンテンツの供給者は経済的に大打撃を被ることになる。

【００１２】本発明の第１の目的は、電子音楽配信を実現するためのインフラストラクチャが未整備であっても、ある音楽コンテンツを購入した消費者に対して、この音楽コンテンツに関連する音楽コンテンツを低価格で尚且つ手軽に販売することができる記録媒体を提供することである。本発明の第２の目的は、著作権保護機構の有無や、暗号鍵の安全性の高低、再生時における音楽コンテンツの再生品質の高低が、再生装置毎に異なる場合であっても、これらに対する音楽コンテンツの配信を一律に行うことができるコンテンツ梱包装置を提供することである。

【００１３】

【課題を解決するための手段】上記第１の目的は、第１コンテンツと、第１コンテンツとは異なるコンテンツであって、第１暗号方式に基づいて暗号化されている第２コンテンツと、第２コンテンツに対応づけられていて、第２コンテンツにおける暗号化を解除させるために用いられる第１鍵情報を含んでおり、所定の装置に予め配布されている第２鍵情報を用いた場合のみ、その暗号化の解除が行われる暗号方式である第２暗号方式にて暗号化されているヘッダとが記録されている記録媒体により達成される。

【００１４】第２の目的は、配布対象を異なる方式にて符号化することにより、再生時の品質が異なるコンテンツを複数得る符号化手段と、再生品質の高低に応じて、各コンテンツをランク付けするランク付け手段と、複数のランクと、各ランクのコンテンツを暗号化するために用いるべき暗号鍵及び暗号アルゴリズムとを組にした対応表を格納する対応表格納手段と、ランクが付与されたコンテンツを、対応表に示されているランクに応じた暗号鍵及び暗号化アルゴリズムを用いて暗号化する暗号化手段と、前記暗号化された複数のコンテンツを含むパッケージを生成する梱包手段とを備えるコンテンツパッケージング装置により達成される。

【００１５】

【発明の実施の形態】本発明に係る記録媒体、再生装置、記録装置についての実施形態について説明する。尚、記録媒体、再生装置、記録装置を一つの実施形態で説明しようとすると説明が著しく煩雑になるので、上記の内容を第１実施形態から第６実施形態において個別に説明するものとする。

【００１６】（第１実施形態）第１実施形態では、音楽コンテンツの販売用途に用いられる記録媒体について説明する。音楽コンテンツの販売用途に用いられる記録媒体には、販売目的の音楽コンテンツが記録されており、この記録媒体が有償で譲渡されることにより、コンテンツの販売がなされる。このような販売用途の記録媒体には、2つのタイプがある。1つ目のタイプは、販売を目的とした音楽コンテンツをEnhanced-CDに記録したものである。Enhanced-CDとは、内周部が通常のCD(CD-DA)と同じ物理構造になっていて、外周部がCD-ROMと同じ物理構造になっておりCD、CD-ROMの両方の機能を兼備したディスクをいう。本Enhanced-CDの外観を図１（ａ）に示し、Enhanced-CDの物理構造を図１（ｂ）に示す。図１

（ａ）においてEnhanced-CDの内周部は、CD-DA部と呼ばれ、外周部は、CD-ROM部と呼ばれる。これら、CD-DA部と、CD-ROM部を機能的に考えると、CD-DA部は、音楽コンテンツ３が記録されているコンテンツ領域１であり、CD-ROM部は、本記録媒体の付加価値を高めるデータを記録した付加価値領域２である。この販売用記録媒体は、このコンテンツ領域１に記録された音楽コンテンツを販売する用途に用いられる。

【００１７】2つ目のタイプの販売用途の記録媒体は、販売目的の音楽コンテンツ３が記録されたDVD-AUDIOである。本DVD-AUDIOの外観を図２（ａ）に示し、その論理フォーマットを図２（ｂ）に示す。このDVD-AUDIOにはEnhanced-CDに示したCD-DA部と、CD-ROM部は存在しないのに対して、販売目的コンテンツ３、再生制御スクリプト４、静止画データ５、コンテナ６のそれぞれがパーソナルコンピュータでアクセス可能なファイルにて記録される。このようにファイルにて記録される点がEnhanced-CDと異なるが、機能的なデータ構造はEnhanced-CD同様であり、コンテンツ領域１と、付加価値領域２とからなる。また、DVD-AUDIOにおけるコンテンツ領域１に音楽コンテンツ３が記録され、付加価値領域２に本記録媒体の付加価値を高めるデータが記録されている点も、Enhanced-CDと同一である。Enhanced-CDとの違いは、Enhanced-CDのコンテンツ領域１には、販売目的コンテンツ３が何の暗号化も施されることなく、そのまま記録されているのに対して、DVD-AUDIOのコンテンツ領域１に記録されている販売目的の音楽コンテンツ３は、DVD-AUDIO固有の識別情報を用いて暗号化されている点である。

【００１８】これらの2つのタイプの販売用記録媒体は、通常のCDと同様、ジャケットや譜面カードを同梱した状態で、専用のプラスチックケースに収納される。図３は、販売用記録媒体を収納した専用のプラスチックケースを示す図である。ここでコンテンツ領域１に記録されているコンテンツの曲名を仮に曲名:○○○とすれば、販売用記録媒体のジャケットには、図３に示すように、曲名:○○○に関する写真が主として印刷されていることがわかる。

【００１９】以上の説明で、コンテンツ領域１、付加価値領域２はEnhanced-CD及びDVD-AUDIOの双方に存在することが明らかになった。続いて、付加価値領域２の記録内容について説明する。図１（ｂ）及び図２（ｂ）の右段に付加価値領域２の記録内容を示す。本図に示すように、付加価値領域２には、再生制御スクリプト４と、静止画データ５と、コンテナ６とが記録されていることがわかる。

【００２０】再生制御スクリプト４は、表示機能付きの装置に本販売用記録媒体が装填された場合、この装置の対話画面に表示させる内容を記述した情報であり、Macromedia Director形式、HTML形式で記述されている。ここでMacromedia Director形式とは、MS-Windows/MacOSの汎用オーサリングソフトの利用時にオーサリング手順の記述に用られる形式であり、HTML形式とは、インターネットブラウザの記述に頻用されている形式である。

【００２１】静止画データ５は、再生制御スクリプト４により再生される対話画面において、表示されるべき静止画像である。これらの再生制御スクリプト４、静止画データ５は、従来のEnhanced-CDにも存在するものであるが、本実施形態における静止画データ５及び再生制御スクリプト４は、従来のものと表示内容が異なる。即ち、従来の静止画データ５及び再生制御スクリプト４には、販売目的コンテンツ３の歌詞やプロモーション映像、ファンクラブや新譜案内等、販売目的コンテンツ３に関連する情報を表示させるものであるが、本実施形態における静止画データ５及び再生制御スクリプト４は、販売目的コンテンツ３とは異なる音楽コンテンツの購入及び再生を推薦する情報を上記装置に表示させる。

【００２２】例えば、販売目的コンテンツ３がある人気アーティストの新譜ならば、本実施形態における再生制御スクリプト４は、その人気アーティストの過去のヒット曲の購入及び再生を推薦している。これら再生制御スクリプト４にて購入及び再生が推薦されている音楽コンテンツが何であるかは、以降の説明で明らかにしてゆく。

【００２３】続いて、Enhanced-CD及びDVD-AUDIOの双方に含まれている付加価値領域２におけるコンテナ６について説明する。コンテナ６のデータ構造は、図４に示すものとなる。本図において、コンテナ６は、暗号化ヘッダ７と、暗号化コンテンツ８とからなり、暗号化ヘッダ７は超流通ヘッダ９を含んでいて、暗号化コンテンツ８は超流通コンテンツ１０を含んでいる。

【００２４】ここで"超流通"とは、筑波大学名誉教授森亮一氏らが唱えるデジタルコンテンツの流通形態である。超流通においてデジタルコンテンツは、予め定められた超流通ヘッダが付与された状態で流通する。この超流通ヘッダには、対価をうるべき権利者を示す対価の詳細に関する対価情報が記されており、消費者がこのデジタルコンテンツの利用を希望した場合、消費者が所有する機器がこれらの権利者情報･対価情報を解釈して使用記録を作成することにより、料金清算を行うのである。

【００２５】超流通ヘッダ９、超流通コンテンツ１０は、このような超流通を前提にした形式、即ち、超流通形式にて、コンテナ６内に収納されている。このように、コンテナ６内に暗号化された状態で収納されている超流通コンテンツ１０こそ、静止画データ５及び再生制御スクリプト４にて、購入及び再生が推薦されている音楽コンテンツである。

【００２６】上述したように超流通ヘッダ９には、権利者情報や対価情報等、超流通を安全に行うために重要な情報が示されているので、これの改竄等の不正行為を効率的に防止する必要がある。そのため、本実施形態にお

ける超流通ヘッダ９は、公開鍵暗号アルゴリズムを応用した暗号方式に基づいて暗号化されたデータ領域を含む（尚、超流通ヘッダ９全体が暗号化されていてもよい。以下の文では、超流通ヘッダ９全体が暗号化されているものとして説明を行う。）。一般に公開鍵暗号には、楕円暗号やRSA暗号(Rivest, Shamir, Adleman encryption)等の種類があることが広く知られている。これら公開鍵を用いて暗号化されたデータを復号するには、暗号化に用いた公開鍵とは異なる復号鍵を用いる必要があるので、公開鍵は、安全性が非常に高いといわれる。

【００２７】しかしながら、本実施形態において超流通ヘッダ９を暗号化する際に用いられる公開鍵応用の暗号方式は、単に公開鍵を用いるだけではなく、以下の点が改良されている。即ち、本実施形態における公開鍵応用の暗号方式では、超流通ヘッダ９内のデータ領域の暗号化を解くための復号鍵が所定の専用装置に予め配布されており、販売用記録媒体がこの専用装置に装填された際に、超流通ヘッダ９の暗号化が解除されるのである。本実施形態においてこの専用装置は、通信回線に接続されており、超流通ヘッダ９の暗号化が解除され、超流通コンテンツが再生されようとする際、又は、超流通コンテンツが他の記録媒体に記録される際、超流通コンテンツについての権利者が正当な対価を得るよう、当該専用装置は、通信回線を介した課金を行うのである。尚、様々な超流通コンテンツを販売用記録媒体に記録させようとする場合、超流通コンテンツのそれぞれの超流通ヘッダについて、異なる公開鍵を用いる。一方、専用装置は、それらの超流通ヘッダが異なる公開鍵を用いて暗号化されていても、共通の復号鍵を用いてこの超流通ヘッダを復号する。また本実施形態において専用装置は、超流通コンテンツを再生又は買い取る際の課金を通信回線を介して行うものとして説明するが、課金情報をICカード等の別の記録媒体に記録しておき、課金情報についての決済を別の装置で行っても良い。また、別の装置にてプリペイドカードによる課金を行ってもよい。

【００２８】超流通ヘッダ９の暗号化を解除するための復号鍵が専用装置に設けられており、販売用記録媒体上に存在しないので、悪意を持った者が販売用記録媒体を取得し、不正な機器を用いてこの超流通ヘッダ９の暗号化を解除しようとしたとしても、その暗号化が解除される確率は極めて低い。このように超流通コンテンツ１０の暗号化を不法に解除するのは極めて困難なので、超流通コンテンツ１０の商取引は、安全に行われる。

【００２９】尚、超流通コンテンツ１０の曲名を△△△とすると、図３に示すように、販売用記録媒体のジャケットには、△△△についての内容は一切印刷されていない。これは、一般の消費者が、「超流通コンテンツ１０は販売目的コンテンツ３を購入した者に無償で供与されるのではないか」と勘違いすることを防止するためである。

【００３０】続いて、超流通ヘッダ９の内容について、図４を参照しながら説明する。図４において最も右側の段は、超流通ヘッダ９の内容を示している。ここからも理解できるように超流通ヘッダ９は、コンテンツID１１、購入条件１２、復号鍵１３から構成されている。コンテンツID１１は、超流通コンテンツ１０を他のコンテンツと識別するための情報が記述されている。超流通コンテンツ１０は音楽コンテンツであるので、ISRC（International Standard Recording Code）等の識別情報がコンテンツID１１として記述される。ここでISRCとは、曲ごとにユニークに割り振られる固有のID情報であって、国コード（２つのASCII文字）、記録年（２桁の数字）、シリアル番号（５桁の数字）により構成される。

【００３１】購入条件１２は、コンテンツの購入条件に関する情報が記述されている。ここで、購入条件１２の一例を図５に示す。図５において「再生許可回数」欄には、再生可能な上限値が整数で記述される。「デジタル出力許可回数」とは、専用装置にデジタル出力端子が備られている場合、このデジタル出力端子を介したデジタル出力を許可するか否かを示し、許可する場合は、その出力回数が整数値で記述される。

【００３２】「再生許可時間」欄は、コンテンツの再生を許可する時間、すなわち再生できる時間が記述される。「再生許可期日」欄は、コンテンツの再生を許可する期日が記述される。再生が許可された期日が過ぎた場合、そのコンテンツの再生はできないことになる。「課金情報」欄は、超流通コンテンツ１０の買い取り時の価格、又は、再生時の価格を示す情報を含む。ここで、買い取り時の価格とは、コンテナ６内の超流通コンテンツ１０を他の記録媒体に記録する際に操作者に課される価格をいい、再生時の価格とは、従量課金、即ち、コンテナ６内の超流通コンテンツ１０の再生回数に応じた価格を表す。この課金情報は、電子商取引において、署名付きの購入申込書として扱われるものであり、これと、操作者IDとを専用装置が課金センタ内のホストコンピュータに送信することは、電子商取引において販売用記録媒体の所有者が超流通コンテンツ１０の購入を申し込むことを意味する。即ち、記録媒体を装填した専用装置は、操作者が超流通コンテンツ１０の再生又は買い取りに合意した場合、通信回線を介して、操作者IDと、この課金情報とを音楽会社の課金センタに送信する。一方、音楽会社の課金センタには、操作者の予めクレジットカード番号が登録されており、このカード番号に対応する銀行口座を予め知得しているので、操作者IDが送信されれば、その送信元の操作者のクレジットカード番号に対応する銀行口座から、課金情報に示される価格を引き落とすことにより、コンテンツの購入代金の決済を行う。

【００３３】復号鍵１３は、超流通コンテンツ１０を復号するための復号鍵である。超流通コンテンツ１０は、LPCM（Linear Pulse Code Modulation）形式、AAC（Adv

anced Audio Coding）形式、DTS（Digital Theater System）形式の音楽コンテンツであり、ブロック暗号方式で暗号化されている。ブロック暗号とは、コンテンツをある一定の長さ（ブロック長）毎に分割して、そのブロック単位で暗号化する方法のことをいい、DES（ブロック長は64bit固定）、RC5（ブロック長は可変）などがこれに相当する。このブロック暗号方式では、暗号化したキーと復号化するための鍵とが同一であるので、公開鍵程、安全性は高く無い。超流通コンテンツ１０の暗号化を解除するには復号鍵１３を入手せねばならないが、復号鍵１３は公開鍵応用の暗号方式で強固に暗号化された超流通ヘッダ９内に存在するので、安全性が高く、超流通コンテンツ１０の暗号化を不法に解除することは非常に困難である。結果として超流通コンテンツ１０は強固に保護されていることになる。

【００３４】このように、超流通コンテンツ１０の購入等に関する購入条件１２は、安全性が高い公開鍵にて暗号化されている超流通ヘッダ９内に含まれているので、課金情報の改竄や超流通ヘッダ９の復号は非常に困難となる。また、超流通コンテンツ１０を公開鍵にて暗号化するのではなく、超流通ヘッダ９のみが公開鍵にて暗号化されているので、超流通コンテンツ１０を得るには、超流通ヘッダ９の暗号化を解除して、復号鍵１３を取り出し、復号鍵１３を用いて超流通コンテンツ１０を解除すればよい。公開鍵応用方式で暗号化されている部分はヘッダ部分に限定されているので、暗号化を解除すべき箇所は短かく、超流通コンテンツ１０の買取や再生を指示してから、買取や再生が可能となる時間は短くて済むので、超流通コンテンツ１０を希望した者を悪戯に苛立たせることはない。この解除に要する時間は、電子音楽配信における音楽コンテンツのダウンロードに要する時間より極めて短くなると考えられるので、操作者は、買取又は再生を希望した超流通コンテンツ１０をすぐさま鑑賞することができる。

【００３５】続いて、販売目的コンテンツ、超流通ヘッダ及び超流通コンテンツについての管理情報について説明する。ここで販売目的コンテンツは、CD、DVD-AUDIOにおける管理情報にて管理されているが、超流通ヘッダ及び超流通コンテンツは、そのような管理情報にて管理されていない。このように販売目的コンテンツは、CD、DVD-AUDIOにおける管理情報にて管理されているため、CDプレーヤ、DVD-AUDIOプレーヤ（これは、後述するデジタルデータ再生装置４００を意味するものではない）により曲として認識され再生されるが、超流通ヘッダ及び超流通コンテンツは、そのような管理情報にて管理されていないため、CDプレーヤ、DVD-AUDIOプレーヤにより曲として認識され再生されることはない。これはCDプレーヤ、DVD-AUDIOプレーヤが、超流通ヘッダ及び超流通コンテンツを、販売目的コンテンツ同様そのまま再生しようとすると、CDプレーヤ、DVD-AUDIOプレーヤは超流通ヘッダ及び超流通コンテンツを復号することができず、無意味で耳障りな音声が出力されてしまうので、そのように超流通ヘッダ及び超流通コンテンツが販売目的コンテンツと同様に再生されることを避けるためである。このようなCD、DVD-AUDIOにおける管理情報に代えて、超流通ヘッダ及び超流通コンテンツには、自身を販売目的コンテンツと区別するための固有の管理情報にて管理されており、専用装置が超流通ヘッダ及び超流通コンテンツを読み出す場合、この固有の管理情報にて、超流通ヘッダ及び超流通コンテンツについての記録開始位置－記録終了位置は特定される。

【００３６】続いて、これら販売目的コンテンツ３及び超流通コンテンツ１０がどのようにして消費者に行き渡るか、超流通コンテンツ１０の超流通がどのように行われるかを図６を参照しながら明らかにしてゆく。図６は、本実施形態における販売目的コンテンツ３と、超流通コンテンツ１０とがどのように流通されるかを示す図である。図６において販売用記録媒体は、矢印y1に示すように音楽会社の直営工場に設置されたデジタルデータ記録装置１００が販売目的コンテンツ３と、再生制御スクリプト４と、静止画データ５と、コンテナ６と、を記録媒体２００に記録することにより、製造される。このようにして製造された販売用記録媒体２００は、通常のCD同様、矢印y2に示すようにトラックの運送等の流通経路を経て、小売り店の店頭で販売される。一般の消費者は、矢印y3に示すように販売されている販売用記録媒体２００を購入することができる。

【００３７】販売用記録媒体２００を購入した消費者は、販売目的コンテンツ３を通常のCD、DVD-AUDIO同様のスタイルで鑑賞することができる。即ち、本図の矢印y4に示すように、歩行中に携帯型の再生装置に再生させることにより、販売目的コンテンツ３を鑑賞することができる。ここで消費者の家庭内には、通信回線に接続された専用装置として、デジタルデータ記録装置３００やデジタルデータ再生装置４００が設置されているものとする。このうちデジタルデータ記録装置３００は、販売用記録媒体２００に記録されている超流通コンテンツ１０を有償で他の記録媒体に記録させるものであり、デジタルデータ再生装置４００は、販売用記録媒体２００に記録されている超流通コンテンツ１０を有償で再生させるものである。また販売用記録媒体２００に記録されている静止画データ５、再生制御スクリプト４は、図８に示す対話画面をこれらデジタルデータ記録装置３００、デジタルデータ再生装置に表示させるものである。図８は、再生制御スクリプト４及び静止画データ５にて再生装置の表示画面に表示される対話画面の一例を示す図である。図８における対話画面は、ライブ演奏の様子等、超流通コンテンツ１０を紹介する画像m1と、超流通コンテンツ１０の再生を推薦する旨のメッセージm2と、その再生に対しての賛同又は拒否を指定できるボタンm3、m1

3と、再生価格の額m4と、当該楽譜の購入を推薦する旨を記述した文字列m5と、その購入に対しての賛同又は拒否を指定できるボタンm6、m16と、その購入価格m7とを含んでおり、超流通コンテンツ１０の有償購入及び有償再生を推薦する内容になっていることがわかる。この対話画面にて、消費者がEnhanced-CDのコンテナ６内にどのような超流通コンテンツ１０が収録されているかを知得し、もしそれらに興味があれば、消費者は、デジタルデータ記録装置３００を用いてこの超流通コンテンツ１０を買い取ることができ、またデジタルデータ再生装置を用いてこの超流通コンテンツ１０を再生させることができる。超流通コンテンツ１０を買い取った際、超流通コンテンツ１０を再生させた際、デジタルデータ記録装置３００、デジタルデータ再生装置４００は、公衆回線を通じて必要な課金額を示す課金情報を送信する。送信された課金情報は、音楽センタの課金センタに設置してあるホストコンピュータ６００に伝送される。

【００３８】図７（ａ）～図７（ｄ）は、デジタルデータ記録装置３００を介して、販売用記録媒体２００から買取用途の記録媒体へのコピーを行う様子を示す図である。ここで買取用途の記録媒体としては、DVD-RAMを用いるものとする。図７（ａ）においてデジタルデータ記録装置３００に販売用記録媒体２００、買取用途の記録媒体６５０がセットされると、図７（ｂ）に示すように、デジタルデータ記録装置３００の操作者は、販売用記録媒体２００に記録されている著作物を買取用途の記録媒体６５０にコピーする。その後、買取用途の記録媒体６５０であるDVD-RAMを図７（ｃ）に示すようにイジェクトすれば、超流通コンテンツ１０の買い取りが完了する。このような買い取り後、DVD-RAMのカートリッジからDVD-RAMを取り出せば、DVD-RAMに記録されたコンテンツは、DVD-RAM対応型のDVD-Audioプレーヤを用いることにより再生される。ここで、DVD-RAM対応型のDVD-Audioプレーヤとは、DVD-Audioディスクのみならず、DVD-RAMの再生を行うことができるDVD-Audioプレーヤをいう。

【００３９】尚、本実施形態では、デジタルデータ記録装置３００は、超流通コンテンツをDVD-RAMに記録したが、メモリカードに記録してもよい。以上のような超流通において、超流通コンテンツ１０に対する課金額は、販売目的コンテンツ３の小売り価格と比較して、割安に設定することができる。何故なら、販売目的コンテンツ３の小売り価格には、Enhanced-CD及びDVD-AUDIOの運送費等、Enhanced-CD及びDVD-AUDIOの流通に係る様々な流通コストが計上されているのに対して、超流通コンテンツ１０の買い取りは、単に暗号化を解除するだけで良く、そのような流通コストが一切不要となるためである。

【００４０】以上のように本実施形態によれば、インターネット等に代表される電子データ配信のためのインフラストラクチャが整備されていない状況にあっても、関連する楽譜の売り込み等、電子音楽配信に近い形態で、対話的な音楽コンテンツの販売を行うことができる。尚、本実施形態では音楽を記録する記録媒体としてEnhanced-CDと、DVD-AUDIOとを用いたが、ハイブリッドタイプのDVD-AUDIO(DVD-AUDIO,DVD-ROMの機能を兼備したディスク)を用いてもよい。更に本実施形態では、販売用途の記録媒体に超流通コンテンツ及び超流通ヘッダを含むコンテナを記録するものとして説明を行ったが、無償配布される記録媒体に超流通コンテンツ及び超流通ヘッダを含むコンテナを記録してもよい。

【００４１】以上で、本発明の記録媒体に記録される第１実施形態、すなわち超流通形式のデータ構造の説明を終わる。

（第２実施形態）第２実施形態は、超流通形式のデータを記録媒体に記録するデジタルデータ記録装置１００に関する。図９に、第２実施形態に係わるデジタルデータ記録装置１００の構成を示す。第２実施形態のデジタルデータ記録装置１００は、汎用のパーソナルコンピュータに専用のアプリケーションプログラムをインストールすることにより実現され、入力部１０１、制御部１０２、エンコード部１０３、コンテンツ格納部１０４、取り出し部１０５、超流通コンテンツ暗号化部１０６、超流通ヘッダ暗号化部１０７、販売目的コンテンツ暗号化部１０８、記録部１０９、固有情報取り出し部１１０を備え、超流通コンテンツを販売用途の記録媒体２００に記録する。以後、これらの構成要素についての説明を行う。

【００４２】なお、本実施形態では、以後、記録対象を音楽コンテンツであるとするが、これに限られるものではなく、映像データや文字データ、あるいはこれらの組み合わせのデータでもよい。また販売用途の記録媒体２００に記録されるべきデータとして、第１実施形態では、再生制御スクリプト４や静止画データ５を例示したが、これらが記録される手順については、本実施形態の主眼と異なるので説明を省略する。

【００４３】入力部１０１は、マウス、キーボード等のポインティングデバイスと接続されており、操作者の指示を受け付ける。ここで、操作者の指示とは、音楽コンテンツのエンコードの指示、あるいは、エンコードしたデータの取り出し要求などが挙げられる。制御部１０２は、入力部１０１の要求を解釈し、音楽コンテンツをエンコードすることを後述するエンコード部１０３へ指示する。あるいは、後述するコンテンツ格納部１０４に記録されている音楽コンテンツを取り出すことを、やはり後述する取り出し部１０５へ指示する。

【００４４】エンコード部１０３は、図示しないマスターテープ等に記録されている原音を例えばLPCM形式のデジタルデータに符号化し、AAC形式に圧縮して音楽コンテンツを生成する。その後第１実施形態に示したコンテ

ンツID１１を生成する。尚、デジタルデータ記録装置１００においてエンコード部１０３は必須ではない。何故なら、外部の業者に音楽コンテンツのエンコードを依頼し、エンコードされたデータをコンテンツ格納部１０４に記録する場合、エンコード部１０３は不必要となるからである。

【００４５】コンテンツ格納部１０４は、大容量のハードディスク装置であって、エンコード部１０３のエンコードにより得られた音楽コンテンツ、及び、第１実施形態に示したコンテンツID１１を格納する。取り出し部１０５は、制御部１０２からの指示に基づいて、エンコードにより得られた音楽コンテンツ並びに第１実施形態に示したコンテンツID１１をコンテンツ格納部１０４から取り出す。

【００４６】超流通コンテンツ暗号化部１０６は、第１実施形態で説明した復号鍵１３を用いて超流通コンテンツ１０を暗号化することにより、暗号化コンテンツ８を生成する。ここで、復号鍵１３は、本デジタルデータ記録装置１００の操作者が自由に設定することができる。超流通ヘッダ暗号化部１０７は、操作者により記述された超流通形式のデータの購入条件１２と、コンテンツID１１と、復号鍵１３とを結合させて超流通ヘッダ９を得て、これを暗号化することにより、暗号化ヘッダ７を得る。さらに、生成した暗号化ヘッダ７を超流通コンテンツ暗号化部１０６が暗号化した暗号化コンテンツ８に付与してコンテナ６を得る。

【００４７】固有情報取り出し部１１０は、販売用記録媒体２００がDVD-AUDIOであり、販売目的コンテンツ３を記録媒体固有の識別情報に基づいて暗号化する必要がある場合、販売用途の記録媒体２００の製造時にあらかじめ記録されている媒体固有の識別情報を取り出し、販売目的コンテンツ暗号化部１０８に出力する。尚、販売用記録媒体２００がEnhanced-CDであり、販売目的コンテンツ３を暗号化する必要がない場合、媒体固有の識別情報を取り出しは行わない。

【００４８】販売目的コンテンツ暗号化部１０８は、販売用記録媒体２００がDVD-AUDIOである場合、販売目的コンテンツ３を、記録媒体固有の識別情報に基づいて暗号化する。尚、販売用記録媒体２００がEnhanced-CDであり、販売目的コンテンツ３を暗号化する必要がない場合、販売目的コンテンツ暗号化部１０８は暗号化を行わない。尚、媒体固有の識別情報に基づいて暗号化する技術については、特開平５－２５７８１６号公報に開示されているので、ここでは詳しい説明は省略する。

【００４９】記録部１０９は、超流通ヘッダ暗号化部１０７により生成されたコンテナ６と、第二の暗号化部１０８で暗号化された販売目的コンテンツとを記録する。以上のように構成されたデジタルデータ記録装置に関して、以後図１０の処理内容を示すフローチャートを用いてその動作を説明する。なお、以下の動作に関しては、すでにエンコード部１０３により、原音のエンコードが完了していて、コンテンツ格納部１０４に複数の音楽コンテンツが得られているものとする。

【００５０】制御部１０２が起動されると、ステップＳ１において制御部１０２は、コンテンツ格納部１０４に格納している複数のコンテンツのうち、販売用途の記録媒体２００に記録すべきものの選択を待つ。コンテンツが選択されれば、ステップＳ２において制御部１０２は操作者からの音楽コンテンツを販売用途の記録媒体２００への記録指示を待つ。ここでの記録指示には、販売を目的として記録する旨の記録指示と、超流通を目的として記録する旨の記録指示とがある。記録指示があった場合、制御部１０２は、ステップＳ３においてそれが販売目的で記録する旨の記録指示か、それとも超流通形式での記録指示かを判定する。

【００５１】操作者が販売用途のコンテンツの記録指示を行った場合、ステップＳ３において、販売用途のコンテンツの記録指示がなされたと判定される。この場合、制御部１０２は、ステップＳ３からステップＳ８に移行し、ステップＳ８において販売用途の記録媒体２００のタイプがDVD-AUDIOであるか、Enhanced-CDであるかを判定する。Enhanced-CDなら、ステップＳ８からステップＳ６に移行して、取り出し部１０５に、選択された音楽コンテンツ及びコンテンツIDの取り出しを指示し、取り出された音楽コンテンツ及びコンテンツIDを販売用途の記録媒体２００に記録させる。一方、DVD-AUDIOなら、ステップＳ８からステップＳ９へと移行する。ステップＳ９において制御部１０２は、取り出し部１０５に、適切な音楽コンテンツ及びコンテンツIDの取り出しを指示すると共に、取り出された音楽コンテンツを販売目的コンテンツ暗号化部１０８に引き渡す。販売目的コンテンツ暗号化部１０８は、販売用途の記録媒体２００からの固有の識別情報の取り出しを、固有情報取り出し部１１０に指示し、これを受けた固有情報取り出し部１１０は、販売用途の記録媒体２００から固有の識別情報を取り出す。その後、ステップＳ９からステップＳ１０に移行して、販売目的コンテンツ暗号化部１０８は、固有情報取り出し部１１０により取り出された媒体固有の識別情報を暗号鍵として用いて暗号化を行なう。その後、ステップＳ１０からステップＳ６に移行し、記録部１０９は、販売目的コンテンツ暗号化部１０８で暗号化された販売目的コンテンツ及びコンテンツIDを販売用途の記録媒体２００に記録する。ステップＳ１からステップＳ６までの処理にて、販売目的コンテンツが販売用途の記録媒体２００が記録されたので、続いて、超流通コンテンツの記録指示がなされた場合の動作について説明する。

【００５２】記録指示が超流通形式であった場合は、制御部１０２は、取り出し部１０５に、選択された音楽コンテンツ及びコンテンツIDを取り出させて、コンテンツIDをヘッダ暗号化部１０７に出力させ、超流通コンテン

ツ暗号化部１０６に出力させる。超流通コンテンツ暗号化部１０６は、ステップＳ４において取り出されたコンテンツを暗号化することにより、暗号化コンテンツを生成する。更に制御部１０２は、ステップＳ５において超流通ヘッダ暗号化部１０７にコンテンツID１１と、購入条件１２と、復号鍵１３とを結合させ、暗号化を行わせることにより、暗号化ヘッダ７を生成させて、暗号化ヘッダ７を暗号化コンテンツ８に付与させることによりコンテナ６を生成する。その後、ステップＳ６に移行して、生成されたコンテナ６を販売用途の記録媒体２００に記録させる。記録媒体への記録が完了すると、ステップＳ７において、記録作業を終了するか否かを操作者に問い合わせ、もし終了するなら、本フローチャートにおける処理を終了する。続行するなら、ステップＳ７からステップＳ１に移行する。以上のように本実施形態によれば、販売用途の記録媒体２００に記録すべき1つ以上のコンテンツのうち、その再生又は他の記録媒体への記録に対価の支払いが必要なものがあればこれを超流通コンテンツ１０として選択して、これを暗号化するので、課金が行われていない間、超流通コンテンツ１０についての再生又は他の記録媒体への記録を防止することができる。

【００５３】超流通コンテンツ１０を暗号化し、超流通コンテンツ１０を再生又は買い取る場合に専用装置に課金を行わせる課金情報と、課金後に専用装置に超流通コンテンツ１０の暗号化を解除させる復号鍵１３とを含む超流通ヘッダ９を超流通コンテンツ１０に付与するので、超流通コンテンツ１０の再生又は他の記録媒体への記録が行われる度に、音楽会社は収益を得ることができる。

【００５４】以上で、第２実施形態の説明を終わる。

（第３実施形態）次に、第３実施形態として、デジタルデータ記録装置３００についての説明を行う。超流通コンテンツ１０の買い取りという側面から、デジタルデータ記録装置３００の内部構成を機能的に記述すれば、デジタルデータ記録装置３００の内部構成は、図１１に示すものとなる。図１１は、第３実施形態のデジタルデータ記録装置３００の内部構成を示す図である。デジタルデータ記録装置３００は、本来電子音楽配信対応型のデジタルデータ記録装置であり、電子音楽配信におけるダウンロード機能、即ち、通信部３１３がコンテンツを有償でインターネットから受信して、買取用途の記録媒体６５０に記録する機能を有している。電子音楽配信対応型であるため、デジタルデータ記録装置３００は、インターネットの通信を行うための通信部や、通信回線において電子商取引を行った場合に、通信回線上で金銭の決済を行うための課金部を有している。

【００５５】図１１において、第３実施形態のデジタルデータ記録装置３００は、一般に汎用のパーソナルコンピュータに専用のアプリケーションプログラムをインストールすることにより実現され、入力部３０１、表示部３０２、制御部３０３、取り出し部３０４、超流通ヘッダ復号化部３０５、超流通コンテンツ復号化部３０６、固有情報取り出し部３０７、超流通コンテンツ再暗号化部３０８、記録部３０９、課金部３１０、課金情報格納部３１２、通信部３１３、及び記録回数管理部３１４を備える。

【００５６】入力部３０１は、マウス、キーボード等のポインティングデバイスと接続されており、操作者からの曲の購入指示を受け付ける。『超流通』における曲の購入とは、『超流通形式のデータを別の記録媒体へ記録する』という行為が含まれる。ここで、デジタルデータ記録装置及びデジタルデータ再生装置にデジタル出力端子が備られている場合、これらのデジタル出力端子にデジタル出力を行わせるという行為も『曲の購入』に含まれる。何故なら、このようなデジタル出力端子に、別の記録媒体のドライブ装置を接続すれば、このドライブ装置を用いて超流通コンテンツ１０をこの記録媒体に記録させることができるからである。本実施形態において、デジタルデータ記録装置１００は、デジタル出力端子を有しており、ケーブルを介してDVD-RAMのドライブ装置を接続している。

【００５７】表示部３０２は、販売用途の記録媒体２００に記録されている再生制御スクリプト４、静止画データ５に基づいて対話画面を表示することにより、超流通コンテンツ１０の内容や、これを購入する際の対価の額等の情報を視覚的に提示する。制御部３０３は、入力部３０１を通じて入力された操作者の指示を解釈し、他の構成要素に指示を行う。あるいは、他の構成要素が出力した結果に応じて、次の処理の指示を行う。例えば、操作者から関連楽譜の購入指示があれば、後述する取り出し部３０４に、販売用途の記録媒体２００に記録されている超流通コンテンツ１０及び超流通ヘッダ９の取り出しを指示する。

【００５８】取り出し部３０４は、第２実施形態に示した販売用途の記録媒体２００に記録されているコンテナ６を取り出す。超流通ヘッダ復号化部３０５は、取り出し部３０４がコンテナ６を取り出すと、それに含まれるコンテナ６内の暗号化ヘッダ７に対して復号鍵１３を用いて復号化を行う。復号により超流通ヘッダ９が得られれば、これに含まれるコンテンツID１１、購入条件１２、復号鍵１３を参照することにより、超流通コンテンツ１０の購入条件を操作者に提示することができる。

尚、超流通ヘッダを復号する際使用する復号鍵は、例えば、デジタルデータ記録装置３００にインストールされるアプリケーションプログラムにあらかじめ格納されているもの、あるいは、通信回線を介して、課金センタから配布されるものを用いる。

【００５９】超流通コンテンツ復号化部３０６は、超流通ヘッダ復号化部３０５が超流通ヘッダ９を復号化すれ

ば、これに含まれる復号鍵１３を用いて、暗号化コンテンツ８を復号化する。固有情報取り出し部３０７は、買取用途の記録媒体６５０から、媒体固有の識別情報を取り出す。ここで買取用途の記録媒体６５０は、DVD-RAMであるので、BCA（Burst Cutting Area）に書かれた情報を媒体固有の識別情報として用いる。この媒体固有の識別情報は、ディスクごとにユニークであり、しかも通常ディスク製作時に記録される情報であって、書き換えることができない。したがって、万一悪意を持った操作者がディスクの内容を複製したとしても、復号鍵のもとになる識別情報が異なるために復号化することができず、データの著作権を確実に保護することが可能となる。

【００６０】超流通コンテンツ再暗号化部３０８は、固有情報取り出し部３０７が取り出した買取用途の記録媒体６５０媒体固有の識別情報に基づき、超流通コンテンツ復号化部３０６が復号化した超流通コンテンツ１０を暗号化する。記録部３０９は、超流通コンテンツ再暗号化部３０８により暗号化された超流通コンテンツ１０を買取用途の記録媒体６５０に記録する。

【００６１】課金部３１０は、記録部３０９の処理の終了通知があると、超流通ヘッダ復号化部３０５が超流通ヘッダ９を復号することにより得られた購入条件１２から、課金情報を読み出して、その課金情報に基づいた課金額を算出し、課金情報に組み入れる。課金情報格納部３１２は、パーソナルコンピュータのハードディスクに相当し、課金部３１０が算出した課金額を含む課金情報を格納する。ここで、課金情報は、悪意を持った操作者が改竄することを防ぐ必要があるので、課金情報は、暗号化した状態でハードディスクに格納したり、ハードディスクにおけるセキュア領域（操作者の通常の操作では、アクセスできない領域）に格納することが望ましい。

【００６２】通信部３１３は、通信回線に接続されたモデム装置と、その制御ソフトウェアとで構成され、課金情報格納部３１２に記録された課金情報と、操作者の操作者IDとを適当なタイミングにおいて、音楽センタの課金センタに設置してあるホストコンピュータ６００に通信回線を介して送信する。ここで、適当なタイミングとは例えば、課金額がある一定値に達したときや、一定の期日に達したときなどが考えられる。勿論、操作者が買取用途の記録媒体６５０に記録するたびにホストコンピュータに接続するとしてもよい。

【００６３】記録回数管理部３１４は、記録部３０９が買取用途の記録媒体６５０に、同一超流通コンテンツ１０を記録した記録回数を記憶しており、記録部３０９が買取用途の記録媒体６５０に同一超流通コンテンツ１０を記録する度に、この記録回数をインクリメントする。以上のように構成されたデジタルデータ記録装置の動作について、以後図１２の処理内容を示すフローチャートを用いて更に詳細に説明する。

【００６４】制御部３０３は、販売用途の記録媒体２００が装填されると、本フローチャートの処理を開始し、ステップＳ２０において関連楽譜の紹介を希望する旨の操作が行われるのを待つ。そのような操作が行われれば、ステップＳ２１において取り出し部３０４がその販売用途の記録媒体２００の付加価値領域２から再生制御スクリプト４及び静止画データ５を読み出して、図８に示した対話画面を表示部３０２に表示させる。その後、ステップＳ２２に移行して、操作者から超流通コンテンツ１０の購入指示が行われるのを待つ。操作者がキャンセル操作を行った場合は、処理を終了するが、購入指示を行った場合、ステップＳ２２からステップＳ２３に移行して、取り出し部３０４に、販売用途の記録媒体２００から、暗号化されたままの暗号化ヘッダ７を含むコンテナ６を取り出させる。その後、ステップＳ２４において、取り出されたコンテナ６における暗号化ヘッダ７を復号化することにより、超流通ヘッダ９を得る。超流通ヘッダ９が得られると、ステップＳ２５において同一超流通コンテンツ１０がこれまで記録された回数を記録回数管理部３１４から読み出す。それと共に、ステップＳ２６において復号により得られた超流通ヘッダ９からデジタル出力許可回数を読み出す。デジタル出力許可回数が読み出されると、ステップＳ２７においてこれまでの記録回数がデジタル出力許可回数に等しいか否かを判定する。もし等しければ、これ以上の超流通コンテンツ１０のデジタル出力は許可し得ないので、そのまま処理を終了する。一方、これまでの記録回数がデジタル出力許可回数を下回るのなら、制御部３０３は、ステップＳ２８において超流通コンテンツ復号化部３０６に超流通ヘッダ９内の復号鍵１３を用いて、コンテナにおける暗号化コンテンツ８を復号化させる。

【００６５】復号が行われると、制御部３０３は、ステップＳ２９において固有情報取り出し部３０７に買取用途の記録媒体６５０から媒体固有の識別情報を取得させ、超流通コンテンツ再暗号化部３０８に、取得した識別情報を暗号鍵としてデータを暗号化させる。その後、ステップＳ３０に移行して、記録部３０９により暗号化されたデータを買取用途の記録媒体６５０に記録させる。

【００６６】記録部３０９による記録が完了すると、ステップＳ３１において制御部３０３は、課金部３１０に購入条件１２中の買い取り価格情報に基づいて、課金額を算出させ、課金情報格納部３１２に課金情報として格納させる。課金情報を格納させた後、ステップＳ３２において課金情報を伝送するのに適当なタイミングが到来するのを待ち、そのようなタイミングが到来すれば、ステップＳ３３において制御部３０３は通信部３１３に、課金情報格納部３１２に記録された課金情報と、操作者IDとを取り出させ、課金センタ内のホストコンピュータ

６００に送信させて、処理を終了する。

【００６７】以上のように本実施形態によれば、販売用途の記録媒体２００を取得した消費者が、この超流通コンテンツ１０の有償での購入に合意した場合のみ、販売用途の記録媒体２００に記録されている超流通コンテンツ１０を買取用途の記録媒体６５０に記録し、この記録行為に対する対価の額を示す課金情報のみを通信回線を介して課金センターに伝送させるので、超流通コンテンツ１０を通信回線に伝送させる必要は無い。故に、通信回線の伝送速度が遅く、電子音楽配信のインフラストラクチャが整備されているとはいえない状態であっても、消費者が負担すべき通信料金は小額で済むので、超流通コンテンツ１０の売買を安価に実現することができる。

【００６８】以上で、第３実施形態の説明を終え、続いて第４実施形態の説明を行う。

（第４実施形態）第４実施形態は、超流通コンテンツの有償での再生を行うデジタルデータ再生装置に関する。本デジタルデータ再生装置４００は、販売用途の記録媒体２００中の超流通形式のデータを他の記録媒体に記録せずに、そのまま復号化して再生する点が第３実施形態で説明したデジタルデータ記録装置３００と大きく異なるが、デジタルデータ再生装置４００は、第３実施形態におけるデジタルデータ記録装置３００同様、電子音楽配信におけるダウンロード機能、即ち、コンテンツを有償でインターネットから受信する機能を有している。そのため、デジタルデータ再生装置は、デジタルデータ記録装置３００と共通の構成要素を多く含んでいる。図１３は、第４実施形態に係るデジタルデータ再生装置の構成を示す図である。図１３におけるデジタルデータ再生装置の構成要素のうち、デジタルデータ記録装置３００と共通の構成要素については、デジタルデータ記録装置３００と同一の参照符号を付して説明を省略する。一方、デジタルデータ再生装置の構成要素のうち４００番台の参照符号を付したもの（再生部４０１、再生回数管理部４０２）は、デジタルデータ記録装置３００が具備していない、デジタルデータ再生装置４００特有の構成要素であり、以降これらの構成要素について説明を行う。

【００６９】図１３における再生部４０１は、超流通コンテンツ復号化部３０６により復号化された超流通コンテンツ１０を再生する。また、超流通コンテンツ１０の再生を開始すると、その旨を課金部３１０に伝える。再生部４０１が再生開始を課金部３１０に伝達することにより、第４実施形態では、超流通コンテンツ１０の再生が行われた際、適切な課金がなされる。

【００７０】再生回数管理部４０２は、再生部４０１が同一の超流通コンテンツ１０を再生した再生回数を記憶しており、再生部４０１が同一の超流通コンテンツ１０を再生する度に、この再生回数をインクリメントする。以上のように構成されたデジタルデータ再生装置の動作について、以後図１４の処理内容を示すフローチャートを用いて更に詳細に説明する。

【００７１】本フローチャートにおいてステップＳ２０からステップＳ２４まで、ステップＳ２８、ステップＳ３１からステップＳ３３までのステップは、図１２の処理内容を示すフローチャートと同一処理である。一方、ステップＳ４１からステップＳ４６までは、第４実施形態特有の処理なのでこれらのステップのみについて説明を行う。ステップＳ２４において、取り出されたコンテナ６における暗号化ヘッダ７が復号化され、超流通ヘッダ９を得ると、ステップＳ４１においてデジタルデータ再生装置の制御部３０３は、同一超流通コンテンツ１０がこれまで再生された回数を再生回数管理部４０２から読み出す。それと共に、超流通ヘッダ９から再生許可回数を読み出す。再生許可回数が読み出されると、ステップＳ４２において制御部３０３は、これまでの再生回数が再生許可回数を下回るか否かを判定し、もし等しければ、これ以上の超流通コンテンツ１０の再生は許可し得ないので、そのまま処理を終了する。

【００７２】これまでの再生回数が再生許可回数を下回るなら、ステップＳ４３において現在日時を読み出し、ステップＳ４４において制御部３０３は、再生許可時間及び再生許可期日を超流通ヘッダ９から読み出す。これらが読み出されると、ステップＳ４５において現在日時が既に再生許可時間及び再生許可期日を経過しているかを判定する。経過していれば処理を終了するが、経過していなければ、ステップＳ４５からステップＳ２８に移行して、超流通コンテンツ復号化部３０６に、超流通ヘッダ９内の復号鍵１３を用いて、コンテナにおける暗号化コンテンツ８を復号化させる。その後、ステップＳ４６において、超流通コンテンツ１０を再生するよう再生部４０１を制御する。

【００７３】以上のように本実施形態によれば、超流通コンテンツ１０の再生開始時に、再生が開始した旨を課金部３１０に伝達するので、超流通コンテンツ１０が再生される度に、音楽会社は収益を得ることができる。

尚、第３実施形態における超流通コンテンツ１０の買い取り機能と、超流通コンテンツ１０の再生機能とを一体化させたデジタルデータ記録装置を構成しても良い。

【００７４】以上で、第４実施形態の説明を終わる。次に第５実施形態の説明を行う。

（第５実施形態）第１実施形態～第４実施形態では、音楽コンテンツが記録媒体を用いて配布されることを想定していたが、第５実施形態では、記録媒体のみならず、インターネットや衛星放送やケーブルTV等の放送波にて音楽コンテンツが配布されることを想定している。図１５は、第５実施形態における音楽コンテンツの配布形態を示す図である。本図において、コンテンツパッケージング装置７００が作成した音楽コンテンツは、DVD-Audio７０１、CD７０２、インターネット７０３、ケーブルT

Ｖ７０４、通信衛星７０５を介して配布されていることを示す図である。一方本図において、コンテンツ再生装置８０１～コンテンツ再生装置８０９は何れも、音楽コンテンツを再生する再生装置であり、音楽コンテンツ再生専用の高級機の再生装置８０１、音楽コンテンツ再生専用であるが低級機の再生装置８０２、８０３、音楽コンテンツ再生専用の携帯型の再生装置８０４、８０５、汎用のパソコンに専用のハードウェアを装着させた再生装置８０６、８０７、衛星放送やCATVの受信用のセットトップボックス型の再生装置８０８、８０９等がある。

【００７５】音楽コンテンツの配布先となる再生装置には、上述したように様々なタイプのものがある。音楽コンテンツ再生専用の民生機器タイプの再生装置８０１、８０２等は、暗号化の解除を行うために専用ハードウェアを具備している。これに対して、汎用パソコン型の再生装置８０６、８０７等は、そのような専用ハードウェアを具備しておらず、汎用ハードウェア上で復号ソフトウェアを動作させることにより、暗号化の解除を行う。これらのことから、汎用パソコンなどは、著作権保護機構が未整備であり、民生機器タイプの再生装置は、著作権保護機構が整備済みであると言える。また、民生機器はコンテンツを再生する際の品質が高く、汎用パーソナルコンピュータはコンテンツを再生する際の品質が低い。故に、コンテンツの再生品質が高い再生装置は著作権保護機構が整備されており、コンテンツの再生品質が低い再生装置は著作権保護機構が未整備であることがわかる。

【００７６】コンテンツパッケージング装置７００及び再生装置８０１～８０９の内部構成を機能的に記述すると、図１６のようになる。図１６は、第５実施形態におけるコンテンツパッケージング装置７００及びコンテンツ再生装置８０１～８０９の内部構成を示す図である。本図において、コンテンツパッケージング装置７００は、コンテンツ符号化部７０６、コンテンツ品質･暗号対応表格納部７０７、コンテンツ暗号化部７０８、コンテンツ梱包部７０９を含む。

【００７７】コンテンツ符号化部７０６は、配布対象を異なる方式にて符号化することにより、再生時の品質が異なるコンテンツを複数得る。この符号化により、販売用コンテンツ７１０と、販売用コンテンツよりも品質の劣る低い品質で再生される試供用コンテンツ７１１とが得られるものとする。コンテンツ品質･暗号対応表格納部７０７は、コンテンツを符号する際の量子化ビット数及びサンプリング周波数と、この量子化ビット数及びサンプリング周波数のコンテンツに付与されるべきランクと対応づけた第１対応表と、各ランクのコンテンツを暗号化するために用いるべき暗号鍵及び暗号アルゴリズムとを組にした第２対応表とを格納する。

【００７８】第１対応表の一例を図１７（ａ）に示す。図１７（ａ）に示すように、第１対応表におけるランク1には、24bitといった量子化ビット数と、96KHzといったサンプリング周波数とが対応づけられており、ランク2には、16bitといった量子化ビット数と、44.1KHzといったサンプリング周波数、ランク3には、16bitといった量子化ビット数と、22.05KHzといったサンプリング周波数とが対応づけられていることがわかる。このように量子化ビット数及びサンプリング周波数が高ければ高い程、対応づけられているランク値は高いことがわかる（ここで、ランク値は、数値が少ない程、ランクが高いことを意味している）。

【００７９】第２対応表の一例を図１７（ｂ）に示す。図１７（ｂ）に示すように、第２対応表におけるランク1には、1024bitといった暗号鍵と、RSAといった暗号化アルゴリズムとが対応づけられており、ランク2には、512bitといった暗号鍵と、RSAといった暗号化アルゴリズム、ランク3には、56bitといった暗号鍵と、DESといった暗号化アルゴリズムとが対応づけられていることがわかる。これらの暗号化アルゴリズムのうち、RSAはDESより安全性が高く、暗号鍵のビット長が長い程、安全性は高いので、このようにランク値が高ければ高い程、対応づけられている暗号鍵及び暗号化アルゴリズムの安全性は高いことがわかる。

【００８０】コンテンツ暗号化部７０８は、再生品質の高低に応じて、各コンテンツをランク付けし、ランクが付与されたコンテンツを、対応表に示されているランクに応じた暗号鍵及び暗号化アルゴリズムを用いて暗号化する。例えば、パッケージの符号化により得られた販売用コンテンツ７１０が配布対象であり、24bitの量子化周波数と、96KHzのサンプリング周波数を有している場合、コンテンツ暗号化部７０８は、図１７（ａ）に示す第１対応表に基づいて、販売用コンテンツ７１０に”1”のランク値を付与する。ランク値を付与した後、コンテンツ暗号化部７０８は、第２対応表における暗号鍵欄を参照して、ランク1に対応する暗号鍵として、1024bitの暗号鍵（セッションキー）を生成する。その後、コンテンツ暗号化部７０８は、第２対応表における暗号化アルゴリズム欄を参照して、当該1024bit長の暗号鍵を公開鍵暗号アルゴリズム（RSA）にて暗号化して、上記スクランブル処理が施された販売用コンテンツに添付する。

【００８１】一方、試供用コンテンツ７１１が配布対象であり、16bitの量子化周波数と、44.1KHzのサンプリング周波数を有している場合、コンテンツ暗号化部７０８は、図１７（ａ）に示す第１対応表に基づいて、販売用コンテンツ７１０に”2”のランク値を付与する。ランク値を付与した後、コンテンツ暗号化部７０８は、第２対応表における暗号鍵欄を参照して、ランク2に対応する暗号鍵として、512bitの暗号鍵（セッションキー）を生成する。その後、コンテンツ暗号化部７０８は、第２対応表における暗号化アルゴリズム欄を参照して、当該512bit長の暗号鍵を公開鍵暗号アルゴリズム（RSA）にて

暗号化して、上記スクランブル処理が施された試供用コンテンツに添付する。

【００８２】コンテンツ梱包部７０９は、コンテンツ暗号化部７０８により暗号化された販売用コンテンツ７１０及び試供用コンテンツ７１１を梱包し、配布形態に応じたパッケージを得る。音楽コンテンツの配布形態がインターネット、衛星放送、CATV等である場合、コンテンツ梱包部７０９は、このパッケージをTCPパケット、トランスポートパケットに変換して出力する。また、音楽コンテンツの配布形態がCD-ROM、DVD-ROMなどの記録媒体である場合、コンテンツ梱包部７０９は、パッケージをUDF形式(ユニバーサルディスクフォーマット)等の形式のファイルに変換して、CD-ROM、DVD-ROMに記録する。このようにパッケージが記録されれば、図１８に示すように、複数のコンテンツを含むパッケージが様々な再生装置に配布されることになる。図１８は、第７実施形態におけるコンテンツ梱包部７０９が梱包を行うことにより得られたパッケージを示す図である。

【００８３】続いてコンテンツ再生装置８０１～８０９について説明する。図１５に示したように、コンテンツ再生装置８０１～８０９は、それぞれ独自の形態を有しているが、図１６に示すハードウェア性能･復号対応表格納部８１０、ハードウェア性能評価部８１１、コンテンツ開梱部８１２、コンテンツ復号化部８１３、コンテンツ格納部８１４、コンテンツ再生部８１５を含む点で共通している。

【００８４】ハードウェア性能･復号対応表格納部８１０は、複数のランク値と、復号鍵及び復号アルゴリズムとを対応づけた対応表を格納している。ここでコンテンツ品質･暗号対応表格納部７０７が格納している第１対応表、第２対応表におけるランク値は、コンテンツにおける再生品質の高低に応じた値を有していたが、ハードウェア性能･復号対応表格納部８１０に格納されている対応表におけるランク値は、再生装置８０１～８０８のそれぞれが有するハードウェア性能を評価するために用いられることに注意されたい。再生装置８０１～８０８のそれぞれが有するハードウェア性能とは、再生装置のハードウェアが、暗号化を復号するために専用ハードウェアを具備しているか否を示し、また著作権保護機構が整備されている場合、その暗号化の解除能力の高さを定量化した値であり、ハードウェア性能のランク値が高い程、その著作権保護機構が整備されていることを示し、ハードウェア性能のランク値が低い程、その著作権保護機構が未整備であることを示す。尚、本実施形態において、ハードウェア性能の評価のためのランク値はランク値A,B,Cという単位を用いて表現し、A→B→Cの順で、ハードウェア性能は高いものとする。図１７（ｃ）は、ハードウェア性能･復号対応表格納部８１０が格納しているハードウェア性能･復号対応表を示す図である。図１７（ｃ）の対応表におけるランクAは、著作権保護機構が整備されていることを示しているが、このランクAには、1024bitといった復号鍵と、RSAといった復号化アルゴリズムとが対応づけられている。一方、ランクB,Cは、ランクAの再生装置と比較して、著作権保護機構が整備されていない再生装置に付与されるべきランク値である。ランク値Bには、56bitといった復号鍵と、RSAといった復号化アルゴリズム、ランクCには、56bitといった復号鍵と、DESといった復号化アルゴリズムとが対応づけられていることがわかる。

【００８５】ハードウェア性能評価部８１１は、コンテンツの暗号化を復号するための専用ハードウェアの具備の有無を検出し、ハードウェアにおいて復号処理に用いることができるメモリ規模を算出することにより、再生装置のハードウェアの性能を評価して、当該ハードウェアの性能を示すランク値を算出する。コンテンツ開梱部８１２は、コンテンツパッケージング装置７００によりパッケージが配布されれば、このパッケージを取得して、このパッケージから販売用コンテンツ、及び試供用コンテンツを抽出する。

【００８６】コンテンツ復号化部８１３は、ハードウェア性能･復号対応表格納部８１０における複数の復号鍵及び復号アルゴリズムのうち、ハードウェア性能評価部８１１により評価されたランク値に応じたものを選択する。それと共に、コンテンツ開梱部８１２により抽出されたコンテンツのうち、選択された復号鍵及び復号アルゴリズムにて暗号化が解除されるべきコンテンツのみを分離して、分離されたコンテンツの暗号化を解除する。

【００８７】ここで上述した民生機器の高級機器であるコンテンツ再生装置８０１が対象である場合、コンテンツ復号化部８１３によるコンテンツの復号がどのように行われるかについて説明する。このコンテンツ再生装置８０１は、暗号化を復号するための専用のハードウェアを有しているので、ハードウェア性能評価部８１１によりハードウェア性能がランクAと評価されることになる。またハードウェア性能･復号対応表格納部８１０においてランクAには、1024bitの復号鍵と、RSAの復号アルゴリズムとが対応づけられているので、コンテンツ復号化部８１３は1024bitの復号鍵と、RSAの復号アルゴリズムとを選択する。一方、販売用コンテンツ７１０は1024bitの暗号化鍵と、RSAの暗号化アルゴリズムを用いて暗号化されているので、コンテンツ復号化部８１３は、コンテンツ開梱部８１２がパッケージから抽出したコンテンツのうち、販売用コンテンツ７１０のみを分離する。そして、公開鍵暗号を解除するために予め配布されている復号鍵を用いて、復号化処理を行う。

【００８８】続いて、汎用ハードウェア上で復号ソフトウェアを動作させることにより、暗号化の解除を行う汎用パーソナルソコンピュータ型のコンテンツ再生装置８０６が対象である場合、コンテンツ復号化部８１３によるコンテンツの復号がどのように行われるかについて説

明する。このコンテンツ再生装置８０６は、汎用のハードウェアしか有していないので、ハードウェア性能評価部８１１によりハードウェア性能がランクCと評価されることになる。一方、ハードウェア性能･復号対応表格納部８１０においてランクCには、56bitの復号鍵と、DESの復号アルゴリズムとが対応づけられているので、コンテンツ復号化部８１３は、56bitの復号鍵と、DESの復号アルゴリズムとを選択する。一方、試供用コンテンツ７１１は56bitの暗号化鍵と、DESの暗号化アルゴリズムを用いて暗号化されているので、コンテンツ復号化部８１３は、コンテンツ開梱部８１２がパッケージから抽出したコンテンツのうち、試供用コンテンツ７１１のみを分離する。一方、DESは、共通鍵暗号なので、暗号化時に用いた暗号鍵により、コンテンツを復号することができる。よって、コンテンツ復号化部８１３は、当該パッケージから暗号鍵を取り出し、これを復号鍵として用いて、復号化処理を行う。

【００８９】コンテンツ格納部８１４は、コンテンツ復号化部８１３により復号されたコンテンツを格納する。コンテンツ再生部８１５は、いったんコンテンツ格納手段７２３に格納された復号済みのコンテンツを再生する。以上のように本実施形態によれば、販売用コンテンツ７１０と、この販売用コンテンツ７１０より低い品質にて再生される試供用コンテンツ７１１とをそれぞれ異なるレベルの暗号化処理を施し、コンテンツ梱包手段７１３によって、パッケージとしてパッケージングするようにしたので、再生側では、ハードウェアの再生性能に応じたコンテンツが選択されて再生されるようになり、音楽コンテンツの配布先の再生装置に、汎用タイプ、高級タイプ等の差違がある場合、これに応じたコンテンツが再生されることになる。そのため、コンテンツを提供する側は、コンテンツの再生環境を考慮することなく、品質の異なるコンテンツを同時に提供することができ、また、コンテンツに対する著作権を安全に保護することができるようになる。

【００９０】以上で第５実施形態の説明を終わる。次に第６実施形態の説明を行う。

（第６実施形態）第６実施形態は、コンテンツ符号化部７０６が、配布対象の先頭部分を符号化することにより試供用コンテンツ７１１を得ると共に、配布対象の残りの部分を符号化することにより販売用コンテンツ７１０を得て、これをパッケージに梱包するというコンテンツパッケージング装置７００の改良に関する。図１９は、第６実施形態における、コンテンツパッケージング装置７００と、コンテンツ再生装置８０１～８０９を示す図である。

【００９１】本実施形態においてコンテンツ暗号化部７０８は、試供用コンテンツに所定のランクを付与し、差分コンテンツに、より高いランクを付与する。ランクが付与されたコンテンツを、対応表に示されているランクに応じた暗号鍵及び暗号化アルゴリズムを用いて暗号化して、コンテンツ梱包部７０９は、前記暗号化された複数のコンテンツを梱包して、パッケージを生成する。図２０は、第７実施形態におけるコンテンツ梱包部７０９が梱包を行うことにより得られたパッケージを示す図である。

【００９２】以上のように本実施形態によれば、コンテンツパッケージング時のパッケージの大きさを縮小することができ、その結果、伝送容量の低減、及びパッケージを記録する、例えば、ハードディスクやCD-ROMなどの記録媒体の容量節約を行うことができる等の利点がある。上記実施形態に基づいて説明してきたが、現状において最善の効果が期待できるシステム例として提示したに過ぎない。本発明はその要旨を逸脱しない範囲で変更実施することができる。代表的な変更実施の形態として、以下（ａ）～（ｆ）に示すものがある。

【００９３】（ａ）第１実施形態～第４実施形態では、買取用途の記録媒体６５０を、DVD-RAMなどの光ディスクとして説明を行なったが、光ディスク以外のハードディスク、半導体メモリなどに置き換えてもよい。

（ｂ）第３～第４実施形態において課金情報を記録するときには、課金情報格納部３１２をパソコンのハードディスクとして説明を行なったが、ハードディスクに限られるものではなく、ICカードなどの記録媒体に置きかえることが可能である。

【００９４】（ｃ）第１～第４実施形態においてデジタルデータ記録装置５００については、パソコンで構成され家庭内で用いられることを想定して説明を行なったが、既存のレコード店などの店舗に設置してもよいことはいうまでもない。

（ｄ）第１～第４実施形態において、情報提供者が提供する情報を音楽コンテンツとして説明したが、これに限るものでなく、音楽コンテンツ、映像コンテンツ、文字情報、あるいは、映像コンテンツと音楽コンテンツと文字情報の組み合わせたものなどでもよいことはもちろんである。

【００９５】（ｅ）第５実施形態において、販売用コンテンツ７１０と、試供用コンテンツ７１１とが配布されるものとしたが、これに限られるものではなく、さらに段階的な品質を有するコンテンツを用いて３つ以上のコンテンツを配信する場合においても適用することができる。

（ｆ）第１～第６実施形態において本実施形態でフローチャートを参照して説明した手順（図１０、図１２、図１４）等を機械語プログラムにより実現し、これを記録媒体に記録して流通･販売の対象にしても良い。このような記録媒体には、ICカードや光ディスク、フロッピーディスク等があるが、これらに記録された機械語プログラムは汎用コンピュータにインストールされることにより利用に供される。この汎用コンピュータは、インスト

ールした機械語プログラムを逐次実行して、本実施形態に示したデジタルデータ記録装置、デジタルデータ再生装置の機能を実現するのである。

【００９６】

【発明の効果】以上説明したように本発明に係る記録媒体は、第１コンテンツと、第１コンテンツとは異なるコンテンツであって、第１暗号方式に基づいて暗号化されている第２コンテンツと、第２コンテンツに対応づけられていて、第２コンテンツにおける暗号化を解除させるために用いられる第１鍵情報を含んでおり、所定の装置に予め配布されている第２鍵情報を用いた場合のみ、その暗号化の解除が行われる暗号方式である第２暗号方式にて暗号化されているヘッダとが記録されているので、第１コンテンツが有名アーティストの新譜であり、第２コンテンツが関連する楽譜であれば、この第１コンテンツを購入した消費者は、第１暗号方式、第２暗号方式の暗号化を解除することにより、この関連する楽譜の音楽コンテンツを入手することができる。この暗号化の解除は、その暗号化を解除させるための第２鍵情報が予め配布されている所定の装置に、本記録媒体を装填すればよいので、消費者は、そのような所定の装置を自宅に有していれば、長時間をかけてコンテンツをダウンロードしなくてもよい。また、第２コンテンツを購入するためにわざわざコンテンツの小売り店に出向かなくてもよい。このように、消費者は、有名アーティストの新譜に関連する楽譜を簡易に入手することができる。

【００９７】また運送費等、記録媒体の流通に係る様々な流通コストは、この記録媒体一枚に対して計上されるので、音楽会社は第２コンテンツに対する課金額は割安に設定することができ、消費者は安価に第２コンテンツを入手することができる。ここで、有償で再生又は買い取りを行うべき第２コンテンツを不正な再生や記録から防御するためには、公開鍵利用のアルゴリズム等、処理負荷が重く、安全性が高いアルゴリズムで第２コンテンツを暗号化せねばならず、第２コンテンツが数メガバイトというデータサイズを有している場合は、その暗号化の解除に要する時間が長時間になることが懸念されるが、本発明に係る記録媒体は、第２コンテンツ自体が第１暗号方式にて暗号化され、ヘッダが第２暗号方式にて暗号化されるので、第２暗号方式が公開鍵利用のアルゴリズムである場合、公開鍵利用のアルゴリズムにて暗号化する箇所を、ヘッダのみに絞ることができる。

【００９８】このように安全性が高いアルゴリズムにて暗号化する箇所をヘッダのみに絞り、その中に第１コンテンツの暗号化を解除するための第１鍵情報を格納しておくので、第２コンテンツ自体を公開鍵利用のアルゴリズムで暗号化する場合と比較して、第２コンテンツにおける暗号化を解除するまでの時間を短くすることができる。これにより超流通コンテンツの買取や再生を指示してから、買取や再生が可能となるまでの時間は短くて済むので、超流通コンテンツの購入を希望した者を悪戯に苛立たせることはなく、購入をキャンセルする確率は低くなる。この解除に要する時間は、電子音楽配信における音楽コンテンツのダウンロードに要する時間より極めて短くなると考えられるので、操作者は、買取又は再生を希望した超流通コンテンツをすぐさま鑑賞することができる。

【００９９】ここで前記所定装置は、課金を行う機能を有しており、前記ヘッダは更に、第２コンテンツの再生又は他の記録媒体への記録を許諾するか否かと、再生又は他の記録媒体への記録を許諾する場合の上限回数とを示す利用制限情報と、第２コンテンツの再生又は他の記録媒体に記録が許諾されている場合に、前記所定装置に課金させるべき再生に要する料金又は他の記録媒体への記録に要する料金を示す課金情報とを含んでいてもも良い。

【０１００】この記録媒体によれば、例えば第２コンテンツが他の記録媒体に記録されることや第２コンテンツが再生されることを無限に許可するのではなく、上限を設定できるので、第２コンテンツの複製が氾濫することや、第２コンテンツの再生が頻繁に行われて第２コンテンツが陳腐化するのを防止することができる。ここで前記所定装置は、課金を行う機能を有しており、前記ヘッダは更に、第２コンテンツの再生又は他の記録媒体への記録を許諾するか否かと、再生又は他の記録媒体に記録を許諾する場合の許可期間を示す許可期間情報と、第２コンテンツの再生又は他の記録媒体に記録が許諾されている場合に、前記所定装置に課金させるべき再生に要する料金又は他の記録媒体への記録に要する料金を示す課金情報とを含んでいてもよい。

【０１０１】この記録媒体によれば、その許可期間情報に示されている期間しか第２コンテンツの複製又は再生を許諾は行なえないので、季節限定、期間限定等のプレミア的な付加価値を第２コンテンツに与えることができる。ここで記録媒体に記録すべきコンテンツを少なくとも1つ以上格納する格納手段と、その再生又は他の記録媒体への記録に課金を行うべきものが前記1つ以上のコンテンツに存在する場合、そのコンテンツを超流通コンテンツとして選択する選択手段と、課金が行われていない間、選択された超流通コンテンツについての再生又は他の記録媒体への記録を防止するよう、第１暗号方式に基づいて超流通コンテンツを暗号化する第１暗号化手段と、超流通コンテンツの暗号化を解除させる鍵情報を含む超流通ヘッダを生成する生成手段と、生成された超流通ヘッダを、前記第１暗号方式より安全性が高い第２暗号方式に基づいて暗号化して、超流通コンテンツに付与する第２暗号化手段と、超流通ヘッダが付与されると、1つ以上のコンテンツをデジタルデータとして記録媒体に記録する記録手段とを備えることを特徴とするデジタルデータ記録装置を用いてもよい。

【０１０２】このデジタルデータ記録装置によれば、販売用途の記録媒体に記録すべき1つ以上のコンテンツのうち、その再生又は他の記録媒体への記録に対価の支払いが必要なものがあればこれを超流通コンテンツとして選択して、これを暗号化するので、課金が行われていない間、超流通コンテンツについての再生又は他の記録媒体への記録を防止することができる。

【０１０３】超流通コンテンツを暗号化し、超流通コンテンツに対する対価を示す課金情報と、対価が支払われた場合に、超流通コンテンツの再生装置に超流通コンテンツの暗号化を解除させるコンテンツキーとを含む超流通ヘッダを超流通コンテンツに付与するので、超流通コンテンツの再生又は他の記録媒体への記録が行われる度に、音楽会社は収益を得ることができる。

【０１０４】ここで第１記録媒体及び第２記録媒体の少なくとも一方を装填する装填手段と、装填手段に装填された記録媒体が第１記録媒体であれば、超流通コンテンツを第１記録媒体から読み出す読出手段と、超流通コンテンツの第２記録媒体への記録に対する対価を操作者に提示する提示手段と、操作者からの操作を受け付ける受付手段と、受付手段が受け付けた操作が、対価の支払いに同意する旨の操作である場合、第１記録媒体から読み出された超流通コンテンツの暗号化を解除する解除手段と、対価の支払いに同意する旨の指示を操作者から受け付けた場合、操作者に対して課金を行う課金手段と、装填手段に超流通コンテンツの記録先となる第２記録媒体が装填されれば、暗号化が解除された超流通コンテンツをデジタルデータとして記録先の第２記録媒体に記録する記録手段とを備えるデジタルデータ記録装置を用いてもよい。

【０１０５】このデジタルデータ記録装置によれば、記録媒体を取得した消費者が、この超流通コンテンツの対価の支払いに合意した場合のみ、記録媒体に記録されている超流通コンテンツを買取用途の記録媒体に記録し、この記録行為に対しての課金を行うので、超流通コンテンツを回線に伝送させる必要は無い。故に、回線の伝送速度が遅く、電子音楽配信のインフラストラクチャが充分整備されているとはいえない状態であっても、消費者が負担すべき通信料金は小額で済むので、超流通コンテンツの売買を安価に実現することができる。

【０１０６】ここで記録媒体を装填する装填手段と、装填手段に装填された記録媒体に超流通コンテンツが記録されていればこれを読み出す読出手段と、超流通コンテンツの再生に対する対価を操作者に提示する提示手段と、操作者からの操作を受け付ける受付手段と、受付手段が受け付けた操作が、対価の支払いに同意する旨の操作である場合、超流通コンテンツの暗号化を解除する解除手段と、対価の支払いに同意する旨の指示を操作者から受け付けた場合、操作者に対して課金を行う課金手段と、暗号化が解除された超流通コンテンツを再生する再生手段とを備えるデジタルデータ再生装置を用いてもよい。

【０１０７】このデジタルデータ再生装置によれば、超流通コンテンツの再生開始時に、課金を行うので、超流通コンテンツが再生される度に、音楽会社は収益を得ることができる。ここで配布対象を異なる方式にて符号化することにより、再生時の品質が異なるコンテンツを複数得る符号化手段と、再生品質の高低に応じて、各コンテンツをランク付けするランク付け手段と、複数のランクと、各ランクのコンテンツを暗号化するために用いるべき暗号鍵及び暗号アルゴリズムとを組にした対応表を格納する対応表格納手段と、ランクが付与されたコンテンツを、対応表に示されているランクに応じた暗号鍵及び暗号化アルゴリズムを用いて暗号化する暗号化手段と、前記暗号化された複数のコンテンツを含むパッケージを生成する梱包手段とを備えるコンテンツパッケージング装置を用いてもよい。

【０１０８】このコンテンツパッケージング装置によれば、販売用コンテンツと、この販売用コンテンツより低い品質にて再生される試供用コンテンツとをそれぞれ異なるレベルの暗号化処理を施し、コンテンツ梱包手段によって、パッケージとしてパッケージングするようにしたので、再生側では、ハードウェアの再生性能に応じたコンテンツが選択されて再生されるようになり、音楽コンテンツの配布先の再生装置に、汎用タイプ、高級タイプ等、様々なタイプが存在する場合、これに応じたコンテンツが再生されることになる。そのため、コンテンツを提供する側は、コンテンツの再生環境を考慮することなく、品質の異なるコンテンツを同時に提供することができ、また、コンテンツに対する著作権を安全に保護することができるようになる。

【０１０９】ここで、配布対象の一部分を符号化することにより試供用コンテンツを得ると共に、配布対象の残りの部分を符号化することにより差分コンテンツを得る符号化手段と、試供用コンテンツに所定のランクを付与し、差分コンテンツに、より高いランクを付与するランク付け手段と、複数のランクと、各ランクのコンテンツを暗号化するために用いるべき暗号鍵及び暗号アルゴリズムとを組にしており、一方の組には、所定のランクが対応づけられ、他方の組みには、当該所定のランクより高いランクに対応づけられている対応表を格納している対応表格納手段と、ランクが付与されたコンテンツを、対応表に示されているランクに応じた暗号鍵及び暗号化アルゴリズムを用いて暗号化する暗号化手段と、前記暗号化された複数のコンテンツを含むパッケージを生成する梱包手段とを備えるコンテンツパッケージング装置を用いてもよい。

【０１１０】このコンテンツパッケージング装置によれば、コンテンツをパッケージングする際のパッケージの大きさを縮小することができ、その結果、伝送容量の低

減、及びパッケージを記録する、例えば、ハードディスクやCD-ROMなどの記録媒体の容量節約を行うことができる等の利点がある。

【図面の簡単な説明】

【図１】（ａ）Enhanced-CDの外観を示す図である。
（ｂ）Enhanced-CDの物理構造を示す図である。

【図２】（ａ）DVD-AUDIOの外観を示す図である。
（ｂ）DVD-AUDIOの機能的なフォーマットを示す図である。

【図３】販売用記録媒体を収納した専用のプラスチックケースを示す図である。

【図４】コンテナ６のデータ構造を示す図である。

【図５】購入条件１２の一例を示す図である。

【図６】本実施形態における販売目的コンテンツ３と、超流通コンテンツ１０とがどのように流通されるかを示す図である。

【図７】（ａ）～（ｄ）販売用記録媒体２００から買取用途の記録媒体６５０へと超流通コンテンツが買い取られる手順を示す図である。

【図８】再生制御スクリプト４及び静止画データ５にて再生装置の表示画面に表示される対話画面の一例を示す図である。

【図９】第２実施形態に係わるデジタルデータ記録装置１００の構成を示す図である。

【図１０】第２実施形態のデジタルデータ記録装置１００の処理内容を示すフローチャートである。

【図１１】第３実施形態のデジタルデータ記録装置３００の内部構成を示す図である。

【図１２】第３実施形態のデジタルデータ記録装置３００の処理内容を示すフローチャートである。

【図１３】第４実施形態のデジタルデータ再生装置４００の内部構成を示す図である。

【図１４】第４実施形態のデジタルデータ再生装置４００の処理内容を示すフローチャートである。

【図１５】第５実施形態における音楽コンテンツの配布形態を示す図である。

【図１６】第５実施形態におけるコンテンツパッケージング装置７００及びコンテンツ再生装置８０１～８０９の内部構成を示す図である。

【図１７】（ａ）第１対応表の一例を示す図である。
（ｂ）第２対応表の一例を示す図である。
（ｃ）ハードウェア性能･復号対応表の一例を示す図である。

【図１８】第５実施形態におけるコンテンツ梱包部７０９が梱包を行うことにより得られたパッケージを示す図である。

【図１９】第６実施形態におけるコンテンツパッケージング装置７００及びコンテンツ再生装置８０１～８０９の内部構成を示す図である。

【図２０】第６実施形態におけるコンテンツ梱包部７０９が梱包を行うことにより得られたパッケージを示す図である。

【符号の説明】

１	コンテンツ領域
２	付加価値領域
３	販売目的コンテンツ
４	再生制御スクリプト
５	静止画データ
６	コンテナ
７	暗号化ヘッダ
８	暗号化コンテンツ
９	超流通ヘッダ
１０	超流通コンテンツ
１１	コンテンツID
１２	購入条件
１３	復号鍵
１００	デジタルデータ記録装置
１０１	入力部
１０２	制御部
１０３	エンコード部
１０４	コンテンツ格納部
１０５	取り出し部
１０６	超流通コンテンツ暗号化部
１０７	超流通ヘッダ暗号化部
１０８	販売目的コンテンツ暗号化部
１０９	記録部
１１０	固有情報取り出し部
２００	販売用途の記録媒体
３００	デジタルデータ記録装置
３０１	入力部
３０２	表示部
３０３	制御部
３０４	取り出し部
３０５	超流通ヘッダ復号化部
３０６	超流通コンテンツ復号化部
３０７	固有情報取り出し部
３０８	超流通コンテンツ再暗号化部
３０９	記録部
３１０	課金部
３１２	課金情報格納部
３１３	通信部
３１４	記録回数管理部
４００	デジタルデータ再生装置
４０１	再生部
４０２	再生回数管理部
５００	通信回線
６００	ホストコンピュータ
６５０	買取用途の記録媒体
７００	コンテンツパッケージング装置
７０６	コンテンツ符号化部

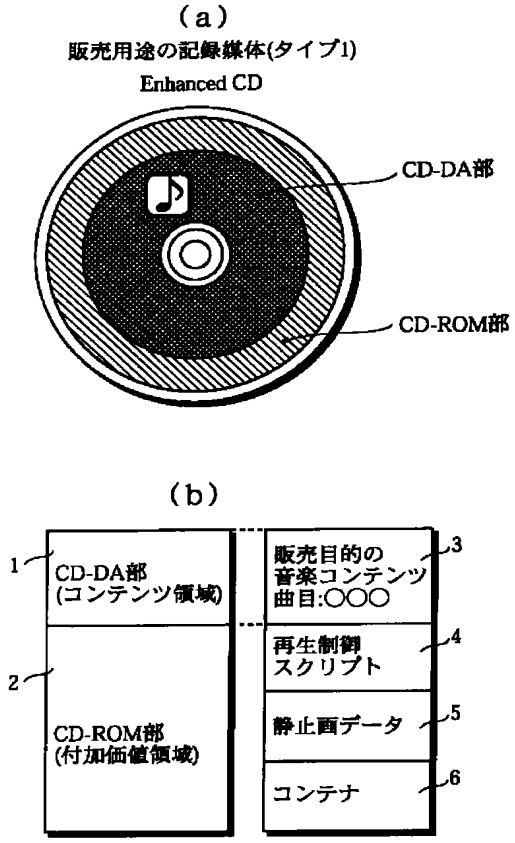
43

７０７　コンテンツ品質･暗号対応表格納部
７０８　コンテンツ暗号化部
７０９　コンテンツ梱包部
７１０　販売用コンテンツ
７１１　試供用コンテンツ
８０１～８０９　コンテンツ再生装置

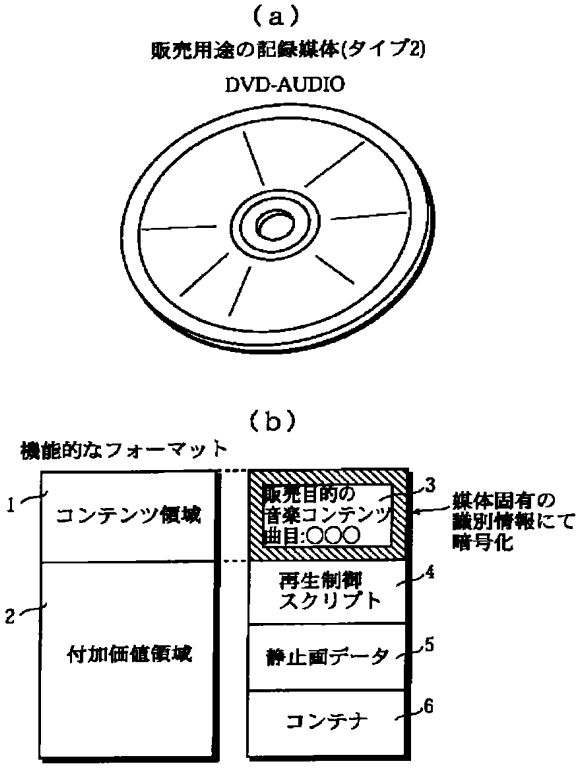
44

＊８１０　ハードウェア性能･復号対応表格納部
８１１　ハードウェア性能評価部
８１２　コンテンツ開梱部
８１３　コンテンツ復号化部
８１４　コンテンツ格納部
＊　８１５　コンテンツ再生部

【図１】

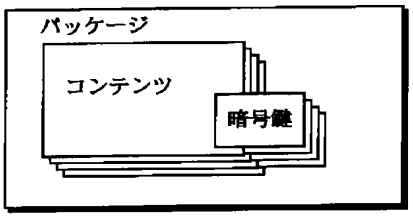


【図２】

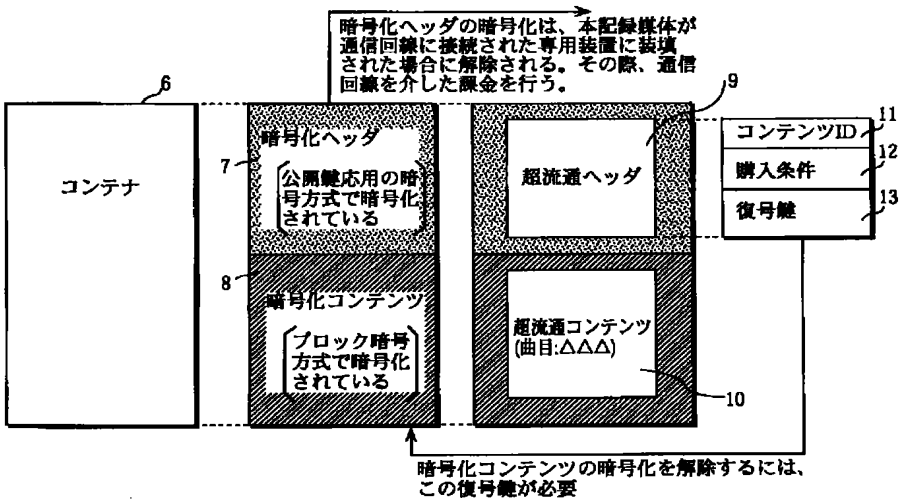


【図３】

【図１８】



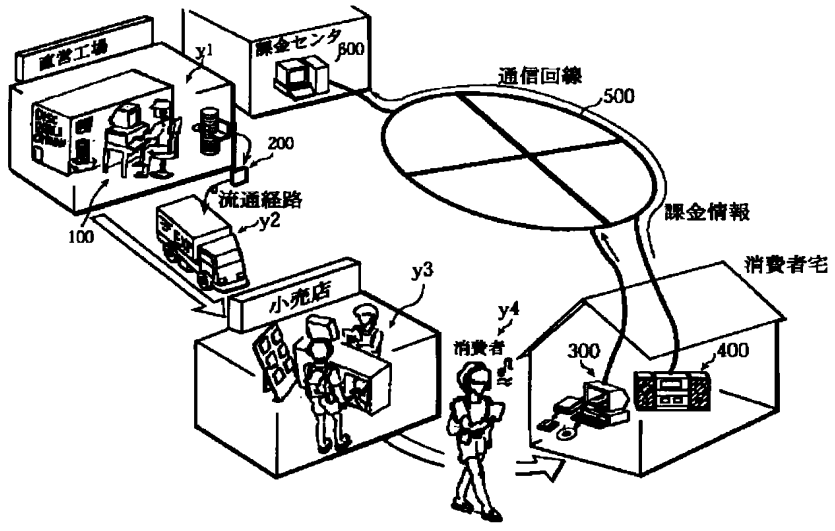
【図４】



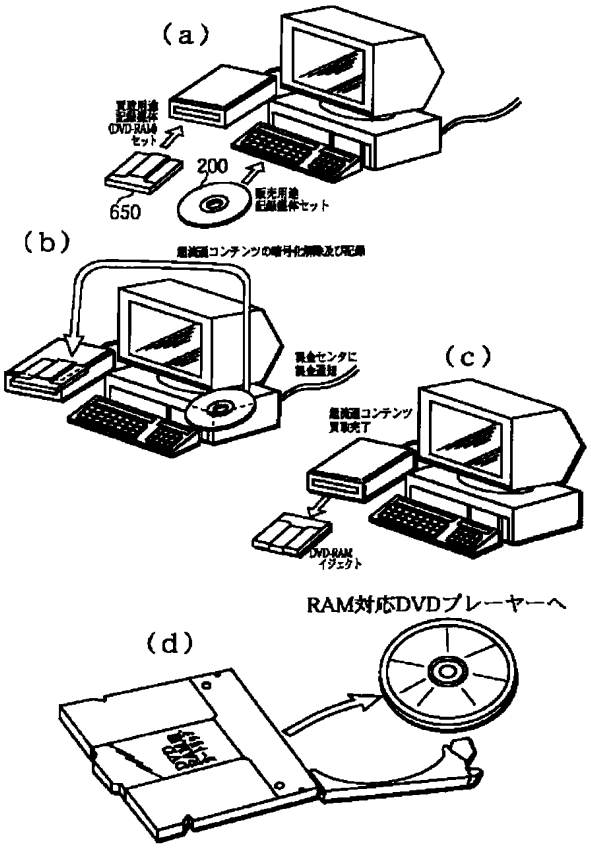
【図５】

名称	内容
再生許可回数	再生可能な回数を記述
ディジタル出力許可回数	ディジタル出力を許可するか否か。許可する場合はその回数を記述
再生許可時間	再生可能な時間を記述
再生許可期日	再生可能な期日を記述
課金情報	買取時の価格や再生回数による使用料金を記述

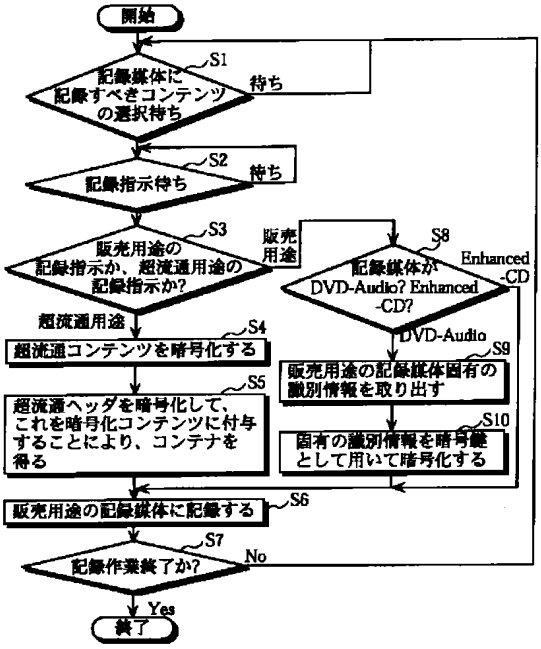
【図６】



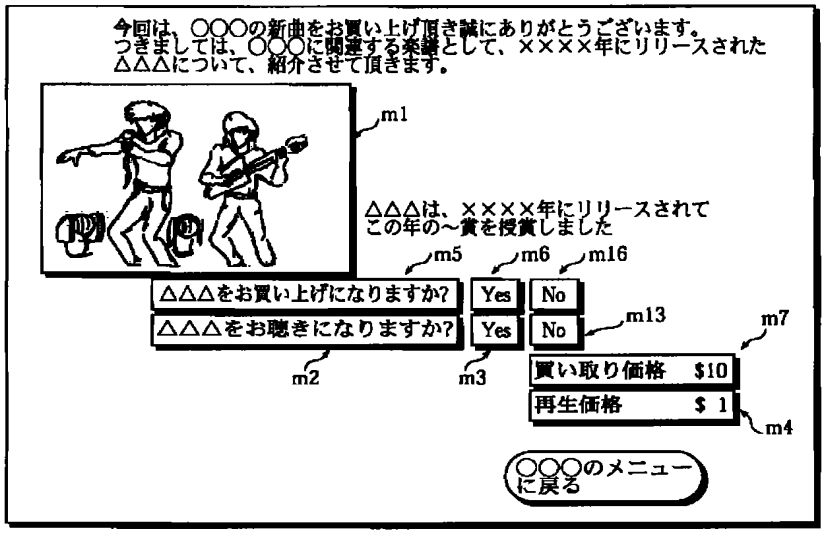
【図７】


(a)
200
650
(b)
(c)
(d)
RAM対応DVDプレーヤーへ

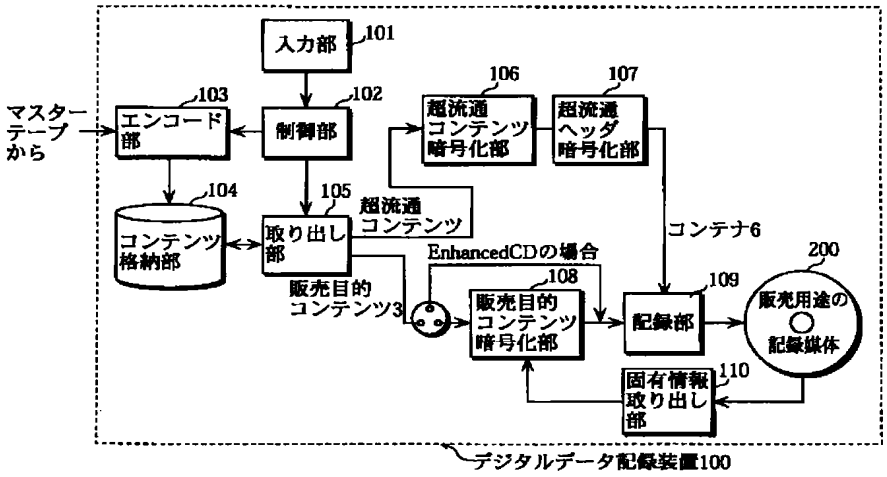
【図１０】


開始
S1
記録媒体に記録すべきコンテンツの選択待ち
待ち
S2
記録指示待ち
待ち
S3
販売用途の記録指示か、超流通用途の記録指示か?
販売用途
超流通用途
S4
超流通コンテンツを暗号化する
S5
超流通ヘッダを暗号化して、これを暗号化コンテンツに付与することにより、コンテナを得る
S6
販売用途の記録媒体に記録する
S7
記録作業終了か?
No
Yes
終了
S8
記録媒体がDVD-Audio? Enhanced-CD?
Enhanced-CD
DVD-Audio
S9
販売用途の記録媒体固有の識別情報を取り出す
S10
固有の識別情報を暗号鍵として用いて暗号化する

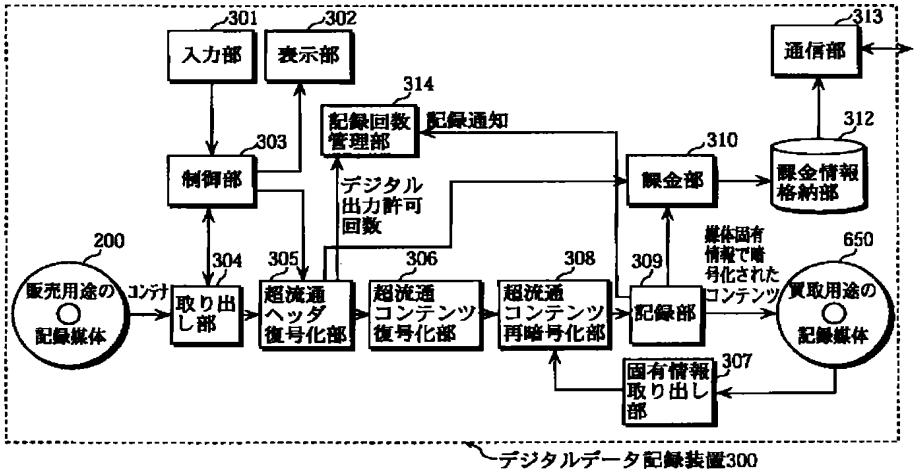
【図８】


今回は、○○○の新曲をお買い上げ頂き誠にありがとうございます。
つきましては、○○○に関連する楽曲として、××××年にリリースされた
△△△について、紹介させて頂きます。
m1
△△△は、××××年にリリースされて
この年の～賞を授賞しました
m5
m6
m16
△△△をお買い上げになりますか?
Yes
No
△△△をお聴きになりますか?
Yes
No
m13
m7
m2
m3
買い取り価格　$10
再生価格　$ 1
m4
○○○のメニューに戻る

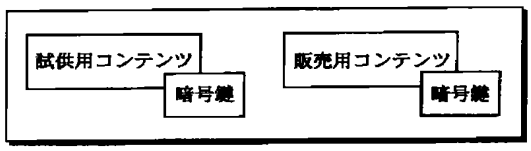
【図９】


入力部
101
マスターテープから
エンコード部
103
制御部
102
106
超流通コンテンツ暗号化部
107
超流通ヘッダ暗号化部
104
コンテンツ格納部
105
取り出し部
超流通コンテンツ
コンテナ6
EnhancedCDの場合
200
販売目的コンテンツ3
108
販売目的コンテンツ暗号化部
109
記録部
販売用途の記録媒体
固有情報取り出し部
110
デジタルデータ記録装置100

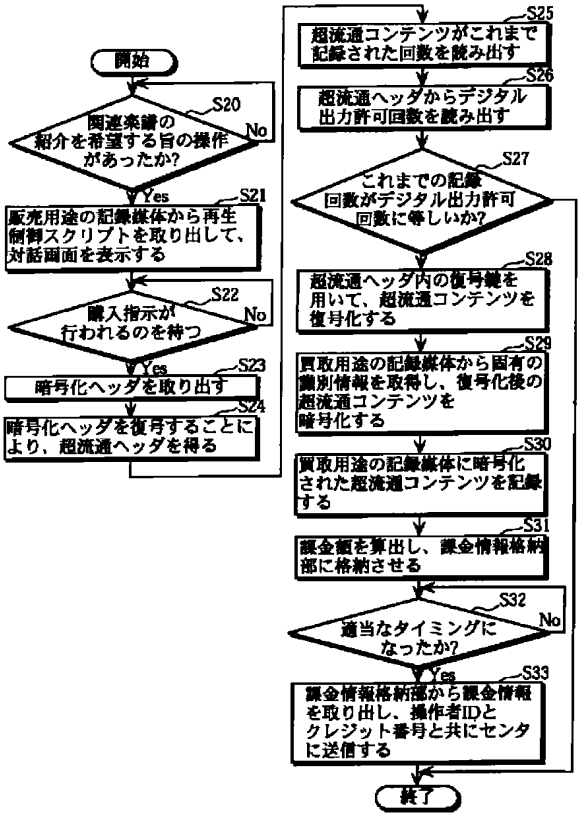
【図１１】


301
入力部
302
表示部
313
通信部
314
記録回数管理部
記録通知
312
303
制御部
310
課金部
課金情報格納部
デジタル出力許可回数
200
販売用途の記録媒体
コンテナ
304
取り出し部
305
超流通ヘッダ復号化部
306
超流通コンテンツ復号化部
308
超流通コンテンツ再暗号化部
309
記録部
媒体固有情報で暗号化されたコンテンツ
650
買取用途の記録媒体
固有情報取り出し部
307
デジタルデータ記録装置300

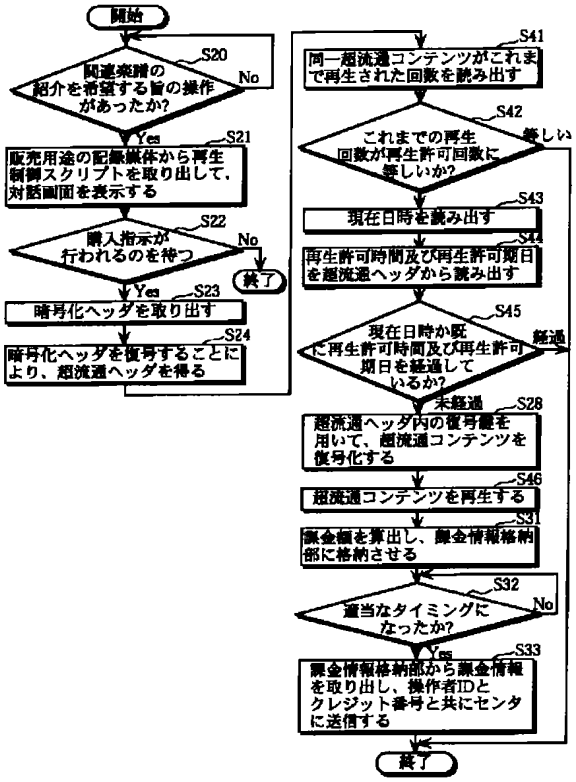
【図２０】


試供用コンテンツ
暗号鍵
販売用コンテンツ
暗号鍵

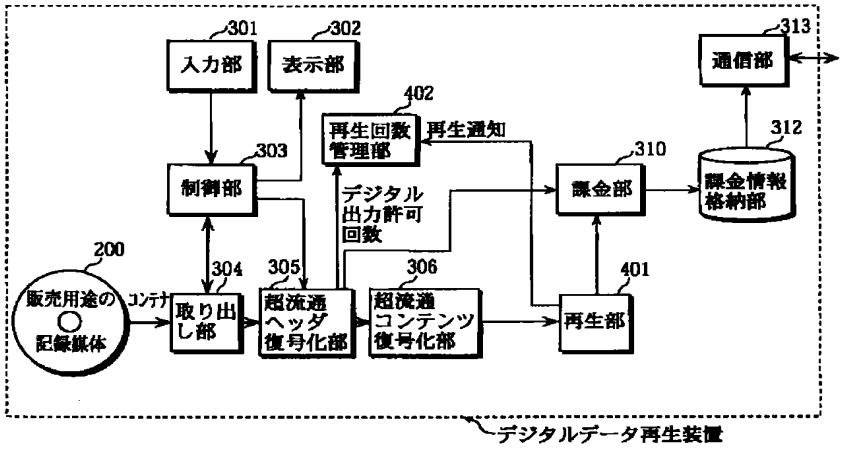
【図１２】


開始
S20
関連楽曲の紹介を希望する旨の操作があったか?
No
Yes
S21
販売用途の記録媒体から再生制御スクリプトを取り出して、対話画面を表示する
S22
購入指示が行われるのを待つ
No
Yes
S23
暗号化ヘッダを取り出す
S24
暗号化ヘッダを復号することにより、超流通ヘッダを得る
S25
超流通コンテンツがこれまで記録された回数を読み出す
S26
超流通ヘッダからデジタル出力許可回数を読み出す
S27
これまでの記録回数がデジタル出力許可回数に等しいか?
S28
超流通ヘッダ内の復号鍵を用いて、超流通コンテンツを復号化する
S29
買取用途の記録媒体から固有の識別情報を取得し、復号化後の超流通コンテンツを暗号化する
S30
買取用途の記録媒体に暗号化された超流通コンテンツを記録する
S31
課金額を算出し、課金情報格納部に格納させる
S32
適当なタイミングになったか?
No
Yes
S33
課金情報格納部から課金情報を取り出し、操作者IDとクレジット番号と共にセンタに送信する
終了

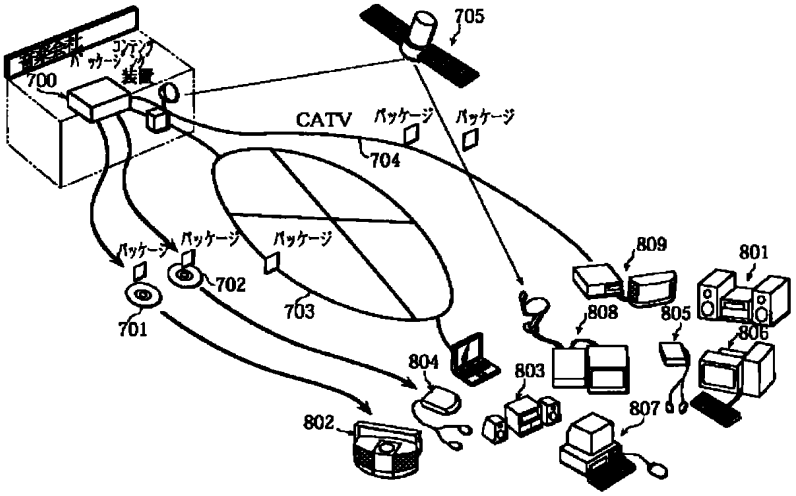
【図１４】


開始
S20
関連楽曲の紹介を希望する旨の操作があったか?
No
Yes
S21
販売用途の記録媒体から再生制御スクリプトを取り出して、対話画面を表示する
S22
購入指示が行われるのを待つ
No
終了
Yes
S23
暗号化ヘッダを取り出す
S24
暗号化ヘッダを復号することにより、超流通ヘッダを得る
S41
同一超流通コンテンツがこれまで再生された回数を読み出す
S42
これまでの再生回数が再生許可回数に等しいか?
等しい
S43
現在日時を読み出す
S44
再生許可時間及び再生許可期日を超流通ヘッダから読み出す
S45
現在日時が既に再生許可時間及び再生許可期日を経過しているか?
経過
未経過
S28
超流通ヘッダ内の復号鍵を用いて、超流通コンテンツを復号化する
S46
超流通コンテンツを再生する
S31
課金額を算出し、課金情報格納部に格納させる
S32
適当なタイミングになったか?
No
Yes
S33
課金情報格納部から課金情報を取り出し、操作者IDとクレジット番号と共にセンタに送信する
終了

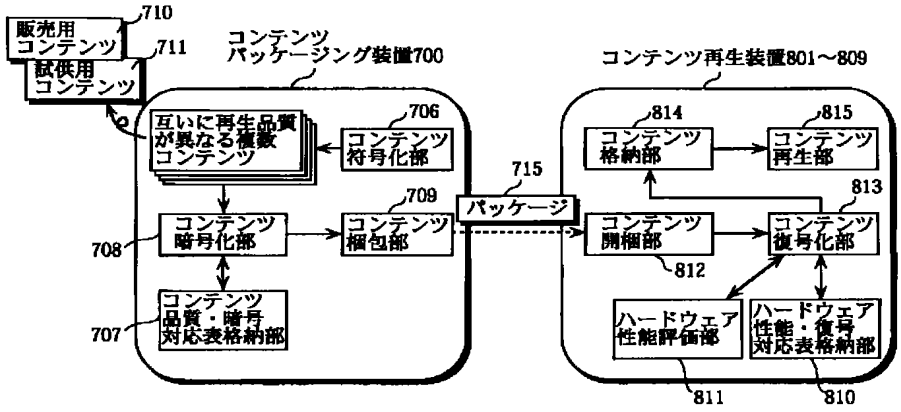
【図１３】


301
入力部
302
表示部
313
通信部
402
再生回数管理部
再生通知
312
303
制御部
310
課金部
課金情報格納部
デジタル出力許可回数
200
販売用途の記録媒体
コンテンツ
304
取り出し部
305
超流通ヘッダ復号化部
306
超流通コンテンツ復号化部
401
再生部
デジタルデータ再生装置

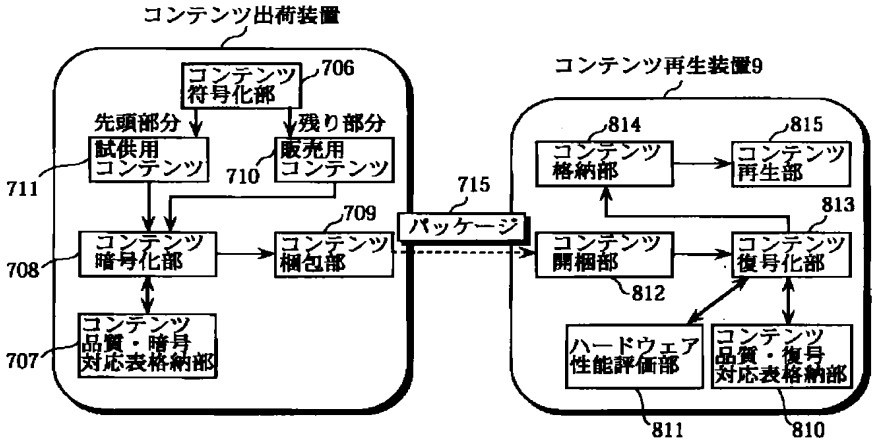
【図１５】


705
コンテンツパッケージ装置
700
CATV
パッケージ
パッケージ
704
パッケージ
パッケージ
パッケージ
702
703
701
809
801
808
805
806
804
803
807
802

【図１６】


710
販売用コンテンツ
711
試供用コンテンツ
コンテンツパッケージング装置700
互いに再生品質が異なる複数コンテンツ
706
コンテンツ符号化部
709
コンテンツ梱包部
715
パッケージ
コンテンツ暗号化部
708
コンテンツ品質・暗号対応表格納部
707
コンテンツ再生装置801～809
814
コンテンツ格納部
815
コンテンツ再生部
813
コンテンツ開梱部
812
コンテンツ復号化部
ハードウェア性能評価部
ハードウェア性能・復号対応表格納部
811
810

【図１９】


コンテンツ出荷装置
コンテンツ符号化部
706
先頭部分
残り部分
試供用コンテンツ
711
販売用コンテンツ
710
715
パッケージ
709
コンテンツ暗号化部
708
コンテンツ梱包部
コンテンツ品質・暗号対応表格納部
707
コンテンツ再生装置9
814
コンテンツ格納部
815
コンテンツ再生部
813
コンテンツ開梱部
812
コンテンツ復号化部
ハードウェア性能評価部
コンテンツ品質・復号対応表格納部
811
810

【図１７】

（ａ）

コンテンツレベル	量子化ビット数	サンプリング周波数
ランク1	24 bit	96 KHz
ランク2	16 bit	44.1 KHz
ランク3	16 bit	22.05 KHz

（ｂ）

コンテンツレベル	暗号鍵	暗号アルゴリズム
ランク1	1024 bit	RSA
ランク2	512 bit	RSA
ランク3	56 bit	DES

（ｃ）

ハードウェア性能レベル	復号鍵	復号アルゴリズム
ランクA	1024 bit	RSA
ランクB	512 bit	RSA
ランクC	56 bit	DES

フロントページの続き

(72)発明者　小塚　雅之
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　青山　昇一
大阪府門真市大字門真1006番地　松下電器産業株式会社内　＊

＊(72)発明者　徳田　克己
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　平田　昇
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(54)【発明の名称】　コンテンツを記録した記録媒体、デジタルデータ記録装置、デジタルデータ再生装置、パッケージを作成するコンテンツパッケージング装置、コンテンツ再生装置、コンピュータ読み取り可能な記録媒体、記録方法、再生方法、パッケージング方法、コンテンツパッケージング装置と、コンテンツ再生装置とからなるシステム。